Bryan Ford

Updated September 4, 2017

EPFL – IC – DEDIS
BC 210, Station 14
CH-1015 Lausanne
Switzerland

Phone: +41 (0)21 693 28 73
Fax: +41 (0)21 693 6610
E-mail: bryan.ford@epfl.ch
Web: http://www.bford.info/

Academic Positions

Associate Professor — 2015–
School of Computer and Communication Sciences — École Polytechnique Fédérale de Lausanne
Research topics: Decentralized/distributed systems, security/privacy, anonymity, anti-censorship.

Associate Professor (tenured 2014) — 2014–2015
Assistant Professor — 2009–2014
Department of Computer Science — Yale University
Research topics: Decentralized/distributed systems, security/privacy, Internet architecture.

Postdoctoral Researcher — 2008–2009
Advisor: Peter Druschel — Max Planck Institute for Software Systems
Research focus: next-generation Internet architecture.

Education

Ph.D. and M.Sc. Computer Science, Massachusetts Institute of Technology, September 2008
Ph.D. Thesis title: *UIA: A Global Connectivity Architecture for Mobile Personal Devices*
M.Sc. Thesis title: *Packrat Parsing: a Practical Linear-Time Algorithm with Backtracking*
Thesis Advisor: M. Frans Kaashoek

B.Sc. Computer Science, University of Utah, June 1998, *summa cum laude*
Thesis Advisor: Jay Lepreau

Courses Taught

Operating Systems (CPSC 422) — Spring '10, '11, '13, '14
Building Decentralized Systems (CPSC 426) — Fall '10, '12, '13, '14
Advanced Systems Topics Seminar (CPSC 722) — Fall '09, '11, '12

Research Supervision

PhD students	*Thesis topic*	*Completion*
Amittai Aviram	Deterministic OpenMP	2012
Michael F. Nowlan	Wire-Compatible TCP for Low-Latency Applications	2014
Ewa Syta	Identity Management through Privacy-Preserving Authentication	2015
Ennan Zhai	Structural Reliability Auditing for Cloud Computing	2015
Weiyi Wu	Deterministically Deterring Timing Channels in Deterland	2015
John Maheswaran	Privacy-Preserving Credentials from Federated Identities	2015

PhD committees	*Institution*	*Thesis topic*	*Completion*
Alexander Vaynberg	Yale U.	Certified Virtual Memory Manager	2012
Yair Sovran	New York U.	Scalable geo-replicated storage	2012
Anton Burtsev	U. Utah	Deterministic systems analysis	2012
Alexander Thomson	Yale U.	Deterministic Database Systems	2013
Andreas Voellmy	Yale U.	Scalable SDN controllers	2014
Hongqiang Liu	Yale U.	Traffic Planning under Network Dynamics	2014
Daniel Winograd-Cort	Yale U.	Effects, Asynchrony, and Choice in AFRP	2015
Sangman Kim	UT Austin	Networking Abstractions for GPU Programs	2015
Shu-Chun Weng	Yale U.	Modular Certified Programming	2015
Mahdi Zamani	U. New Mexico	Scalable Anonymous Communication	2016
Iris Safaka	EPFL	Unconditional security and privacy	2016
Rafik Chaabouni	EPFL	Set Membership and Range Proofs	2016
Maxime Augier	EPFL	Trustworthy Cloud Storage	2016
Berker Ağir	EPFL	Context and semantic aware location privacy	2016
Hao Zhuang	EPFL	Multicloud Resource Allocation	2016
Arthur Gervais	ETHZ	Proof of Work Blockchains	2016

Postdocs and Resarch Scientists	*Research topic*	*Period*
Syed Obaid Amin	Next-generation Transport Services	2009–2012
David Isaac Wolinsky	Disruption-Proof Anonymous Communication	2011–2015
Philipp Jovanovic	Scalable, Transparent Decentralized Systems	2015–
Stevens Le Blond	Mobile Operating System Security and Privacy	2017–

External Research Funding

DHS grant FA8750-16-2-0034: *PriFi Networking for Tracking Resistant Mobile Computing,* Joan Feigenbaum (PI), David Isaac Wolinsky, and Bryan Ford (co-PIs). Feb 2016–Jan 2019, $1,727,334.

AXA Research Program: *Privacy-Preserving Decentralized Systems and Emergent Risks from Big Data Computing,* Bryan Ford (PI). Sep 2015–2025, CHF 1,500,000.

NSF TWC-1409599: *Hiding Hay in a Haystack: Integrating Censorship Resistance into the Mainstream Internet,* Vitaly Shmatikov (PI) and Bryan Ford (co-PI). Sep 2014–Aug 2018, $600,000.

NSF CNS-1407454: *An App-Centric Transport Architecture for the Internet,* Hari Balakrishnan (PI) and Bryan Ford (co-PI). Sep 2014–Aug 2018, $399,999.

Cisco University Research Grant, *The Minion Suite: A Network-Compatible Datagram Substrate for Internet Applications and Transports,* Janardhan Iyengar (PI) and Bryan Ford. Sep 2012, $98,999.

NSF CNS-1149936: *CAREER: From Storm Clouds to EverCouds: Heading Off Long-Term Cloud Computing Risks,* Bryan Ford (PI). Jun 2012–May 2016, $450,000.

ONR award N000141210478: *Reasoning Infrastructure for Security-Aware Software Development,* Bryan Ford (PI), Joan Feigenbaum, and Zhong Shao. Apr 2012–Mar 2015, $750,000.

NSF CNS-1065451: *Making OS Kernels Crash-Proof by Design and Certification,* Zhong Shao (PI) and Bryan Ford. Aug 2011–Jul 2015, $1,116,262.

DARPA SAFER contract N66001-11-C-4018: *Dissent: Scalable and Disruption-Proof Anonymity for Interactive Internet Communication,* Bryan Ford (PI), Joan Feigenbaum, and Vitaly Shmatikov. Dec 2010–Oct 2014, $3,699,999.

DARPA CRASH award FA8750-10-2-0254: *Advanced Development of Certified OS Kernels,* Zhong Shao (PI) and Bryan Ford. Oct 2010–Sep 2014, $2,657,704.

NSF CNS-1017206: *An Operating System and Programming Model for Deterministic Parallel Computation,* Bryan Ford (PI). Aug 2010–Jul 2013, $472,130.

ONR grant N00014-09-10757: *Proactively Removing the Botnet Threat,* Joan Feigenbaum (PI), Steven M. Bellovin, Angelos Keromytis Salvatore J. Stolfo, Vitaly Shmatikov, Michael Walfish, and Bryan Ford. Apr 2009–Sep 2010, $883,627.

NSF CNS-0916413: *Tng, a Next Generation Transport Services Architecture,* Bryan Ford (PI) and Janardhan Iyengar. Aug 2009–Jul 2011, $328,260.

Outreach Activities

Broader-audience and popular media writing (selected)		*Year*
Seeking Anonymity in an Internet Panopticon	*Communications of the ACM*	2015
GPUfs: the case for operating system services on GPUs	*Communications of the ACM*	2014
Technology Can Make Lawful Surveillance Open and Effective	*MIT Technology Review*	2014
Is Data Hoarding Necessary for Lawful Surveillance?	*Huffington Post*	2014

Technology blogging		*Year*
Guest post: Apple, FBI, and Software Transparency	Freedom to Tinker	2016
Personal blog	Bryan Ford	2002–

Technology standardization activities	*Year*
IETF and IRTF security and cryptography working groups	2015–
IETF transport and NAT working groups (co-authored 4 RFCs)	2005–2010

Work drawing popular media coverage	*Year*	
Riffle anonymity system	20+ articles in multiple languages	2016
Apple, FBI, and Software Transparency blog post	10+ articles and radio interviews	2016
Open letter opposing mass surveillance	4+ articles	2014
Dissent anonymity system	5+ articles	2013–2016
Icebergs in the Clouds workshop paper	15+ articles in multiple languages	2010
Deterministic timing channel control paper	1 article	2010

Technology consulting		*Year*
SICPA	Cryptocurrencies and blockchain technology	2015
Nuvoiz	NAT traversal technology for VoIP	2006

Scientific Service Activities

Conference and workshop program committees	*Year*
BPASE	2018
PETS, ASPLOS ERC, BITCOIN, IEEE S&B	2017
OSDI, PLDI, PETS, WWW	2016
SOSP, IEEE S&P, SIGCOMM, SAT, RAID	2015
OSDI, EuroSys, APSys, FOCI	2014
SOSP, ASPLOS, NSDI, WWW, SYSTOR	2013
EuroSys, CCS, ASPLOS ERC, WoDet, CCSW	2012
SOSP, USENIX, CCS, CCSW, MobiHeld	2011
OSDI, HotNets	2010
IMC, NPSec, ICCCN	2009
ROADS	2008

Program committee chairing	*Year*
USENIX ATC	2017
HotNets	2016
WoDet, SOSP Poster/WIP	2011
PFLDnet	2010

US National Science Foundation (NSF) review panelist	2010, 2011, 2013, 2014

DARPA Information Science and Technology (ISAT) study organizer	*Year*
The EverCloud: Anticipating and Countering Cloud-Rot	2014
Technological Disruptions of Societies and Organizations	2016
Technologies for Scalable Self-Organizing Communities	2017

Invited lectures (selected)	*Year*
International School on Foundations of Security Analysis and Design (FOSAD)	2016
Keynotes at SYSTOR, FCS, Italian AXA Forum	2016
Keynote at ICISSP conference	2015
Dissent project: invited talks at 10+ research institutions	2011–2015
Privacy vs. Security policy panelst at George C. Marshall Institute, Washington, D.C.	2014
Keynote at NDSS SENT workshop	2014

Selected Awards and Distinguished Memberships

AXA Research Fund Chair in Information Security and Privacy, 2015.

DARPA Information Science and Technology (ISAT) Advisory Group, 2014–2017.

NSF Faculty Early Career Development (CAREER) Award, 2012.

Jay Lepreau Best Paper award, Operating Systems Design and Implementation (OSDI), 2010.

Best Student Paper award, USENIX Annual Technical Conference, 2008.

Presidential Fellowship, Massachusetts Institute of Technology, 2000.

Inaugural Computing Research Association Outstanding Undergraduate Award, 1995.

Barry M. Goldwater Excellence in Education scholarship, 1994.

Clyde Christensen College of Engineering scholarship, Univeristy of Utah, 1991.

Refereed Journal Publications

1. *Riffle: An Efficient Communication System With Strong Anonymity*, Albert Kwon, David Lazar, Srinivas Devadas, and Bryan Ford. *Proceedings of Privacy Enhancing Technologies* 2016(2), December 2015.
2. *Security Analysis of Accountable Anonymity in Dissent*, Ewa Syta, Aaron Johnson, Henry Corrigan-Gibbs, Shu-Chun Weng, David Wolinsky, and Bryan Ford. *ACM Transactions on Information and System Security (TISSEC)* 17(1), August 2014.
3. *GPUfs: Integrating a File System with GPUs*, Mark Silberstein, Bryan Ford, Idit Keidar, and Emmett Witchel. *ACM Transactions on Computing Systems (TOCS)* 32(1), February 2014.
4. *A Dynamic Recursive Unified Internet Design (DRUID)*, J. Touch, I. Baldine, R. Dutta, G. Finn, B. Ford, S. Jordan, D. Massey, A. Matta, C. Papadopoulos, P. Reiher, and G. Rouskas. Computer Networks 55(4), March 2011.

Refereed Conference Publications

1. *Atom: Horizontally Scaling Strong Anonymity*, Albert Kwon, Henry Corrigan-Gibbs, Srinivas Devadas, and Bryan Ford. ACM Symposium on Operating Systems Principles (SOSP), October 2017.
2. *CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds*, Kirill Nikitin, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Nicolas Gailly, Linus Gasser, Ismail Khoffi, Justin Cappos, and Bryan Ford. USENIX Security Symposium, August 2017.
3. *Scalable Bias-Resistant Distributed Randomness*, Ewa Syta, Philipp Jovanovic, Eleftherios Kokoris Kogias, Nicolas Gailly, Linus Gasser, Ismail Khoffi, Michael J. Fischer, and Bryan Ford. IEEE Security & Privacy, May 2017.
4. *Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing*, Eleftherios Kokoris Kogias, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser, and Bryan Ford. USENIX Security Symposium, August 2016.

5. *Keeping Authorities "Honest or Bust" with Decentralized Witness Cosigning*, Ewa Syta, Iulia Tamas, Dylan Visher, David Isaac Wolinsky, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ismail Khoffi, and Bryan Ford. IEEE Security & Privacy, May 2016.
6. *AnonRep: Towards Tracking-Resistant Anonymous Reputation*, Ennan Zhai, David Isaac Wolinsky, Ruichuan Chen, Ewa Syta, Chao Teng, and Bryan Ford. NSDI 2016, March 2016.
7. *Building Privacy-Preserving Cryptographic Credentials from Federated Online Identities*, John Maheswaran, Daniel Jackowitz, Ennan Zhai, David Isaac Wolinsky, and Bryan Ford. CODASPY 2016, March 2016.
8. *Deterministically Deterring Timing Attacks in Deterland*, Weiyi Wu and Bryan Ford. TRIOS 2015, October 2015.
9. *Private Eyes: Secure Remote Biometric Authentication*, Ewa Syta, Michael J. Fischer, David Wolinsky, Abraham Silberschatz, Gina Gallegos-Garcia, and Bryan Ford. SECRYPT 2015, July 2015.
10. *Heading Off Correlated Failures through Independence-as-a-Service*, Ennan Zhai, Ruichuan Chen, David Isaac Wolinsky, and Bryan Ford. OSDI 2014, October 2014.
11. *Managing NymBoxes for Identity and Tracking Protection*, David Isaac Wolinsky, Daniel Jackowitz, and Bryan Ford. TRIOS 2014, October 2014.
12. *TAQ: Enhancing Fairness and Performance Predictability in Small Packet Regimes*, Jay Chen, Lakshmi Subramanian, Janardhan Iyengar, and Bryan Ford. EuroSys 2014, April 2014.
13. *Hang With Your Buddies to Resist Intersection Attacks*, David Isaac Wolinsky, Ewa Syta, and Bryan Ford. 20th ACM Conference on Computer and Communications Security, November 2013.
14. *Ensuring High-Quality Randomness in Cryptographic Key Generation*, Henry Corrigan-Gibbs, Wendy Mu, Dan Boneh, and Bryan Ford. 20th ACM Conference on Computer and Communications Security, November 2013.
15. *Proactively Accountable Anonymous Messaging in Verdict*, Henry Corrigan-Gibbs, David Isaac Wolinsky, and Bryan Ford. 22nd USENIX Security Symposium, August 2013.
16. *Maple: Simplifying SDN Programming Using Algorithmic Policies*, Andreas Voellmy, Junchang Wang, Y. Richard Yang, Bryan Ford, and Paul Hudak. ACM SIGCOMM, August 2013.
17. *GPUfs: Integrating a File System with GPUs*, Mark Silberstein, Bryan Ford, Idit Keidar, and Emmett Witchel. 18th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), March 2013.
18. *Enhancing the OS Against Security Threats in System Administration*, Nuno Santos, Rodrigo Rodrigues, and Bryan Ford. 2012 ACM/IFIP/USENIX International Middleware Conference (Middleware), December 2012.
19. *Dissent in Numbers: Making Strong Anonymity Scale*, David Isaac Wolinsky, Henry Corrigan-Gibbs, Bryan Ford, and Aaron Johnson. 10th USENIX Symposium on Operating Systems Design and Implementation (OSDI), October 2012.
20. *Fitting Square Pegs Through Round Pipes: Unordered Delivery Wire-Compatible with TCP and TLS*, Michael Nowlan, Nabin Tiwari, Janardhan Iyengar, Syed Obaid Amin, and Bryan Ford. 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI), April 2012.
21. *Eyo: Device-Transparent Personal Storage*, Jacob Strauss, Justin Mazzola Paluska, Chris Lesniewski-Laas, Bryan Ford, Robert Morris, and Frans Kaashoek. USENIX Annual Technical Conference, June 2011.
22. *Efficient System-Enforced Deterministic Parallelism*, Amittai Aviram, Shu-Chun Weng, Sen Hu, and Bryan Ford. *Winner of Jay Lepreau Best Paper Award.* 9th USENIX Symposium on Operating Systems Design and Implementation (OSDI), October 2010.
23. *Dissent: Accountable Anonymous Group Messaging*, Henry Corrigan-Gibbs and Bryan Ford. 17th ACM Conference on Computer and Communications Security (CCS), October 2010.

24. *Vx32: Lightweight User-level Sandboxing on the x86*, Bryan Ford and Russ Cox. USENIX Annual Technical Conference (USENIX), June 2008. *Awarded Best Student Paper.*
25. *Alpaca: Extensible Authorization for Distributed Services*, Christopher Lesniewski-Laas, Bryan Ford, Jacob Strauss, M. Frans Kaashoek, and Robert Morris. 14th ACM Symposium on Computer and Communications Security (CCS), October 2007.
26. *Structured Streams: a New Transport Abstraction*, Bryan Ford. ACM SIGCOMM, August 2007.
27. *Persistent Personal Names for Globally Connected Mobile Devices*, Bryan Ford, Jacob Strauss, Chris Lesniewski-Laas, Sean Rhea, Frans Kaashoek, and Robert Morris. 7th USENIX Symposium on Operating Systems Design and Implementation (OSDI), November 2006.
28. *VXA: A Virtual Architecture for Durable Compressed Archives*, Bryan Ford. 4th USENIX Conference on File and Storage Technologies (FAST), December 2005.
29. *Peer-to-Peer Communication Across Network Address Translators*, Bryan Ford, Pyda Srisuresh, and Dan Kegel. USENIX Annual Technical Conference (USENIX), April 2005.
30. *Parsing Expression Grammars: A Recognition-Based Syntactic Foundation*, Bryan Ford. 31st ACM Symposium on Principles of Programming Languages (POPL), January 2004.
31. *Packrat Parsing: Simple, Powerful, Lazy, Linear Time*, Bryan Ford. International Conference on Functional Programming (ICFP), October 2002.
32. *Interface and Execution Models in the Fluke Kernel*, Bryan Ford, Mike Hibler, Jay Lepreau, Roland McGrath, and Patrick Tullmann. USENIX Symposium on Operating Systems Design and Implementation (OSDI), February 1999.
33. *The Flux OSKit: A Substrate for Kernel and Language Research*, Bryan Ford, Godmar Back, Greg Benson, Jay Lepreau, Albert Lin, and Olin Shivers. 16th ACM Symposium on Operating System Principles (SOSP), October 1997.
34. *Flick: A Flexible, Optimizing IDL Compiler*, Eric Eide, Kevin Frei, Bryan Ford, Jay Lepreau, Gary Lindstrom. ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI), June 1997.
35. *Microkernels Meet Recursive Virtual Machines*, Bryan Ford, Mike Hibler, Jay Lepreau, Patrick Tullmann, Godmar Back, and Stephen Clawson. USENIX Symposium on Operating Systems Design and Implementation (OSDI), October 1996.
36. *CPU Inheritance Scheduling*, Bryan Ford and Sai R. Susarla. USENIX Symposium on Operating Systems Design and Implementation (OSDI), October 1996.
37. *Evolving Mach 3.0 to a Migrating Thread Model*, Bryan Ford and Jay Lepreau. USENIX Winter Technical Conference (USENIX), January 1994.
38. *In-Kernel Servers on Mach 3.0: Implementation and Performance*, Jay Lepreau, Mike Hibler, Bryan Ford, and Jeffrey Law. 3rd USENIX Mach Symposium, April 1993.

Refereed Workshop Publications

39. *Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies*, Maria Borge, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, and Bryan Ford. IEEE Security & Privacy on the Blockchain (IEEE S&B), April 2017.
40. *Privacy-Preserving Lawful Contact Chaining*, Aaron Segal, Joan Feigenbaum, and Bryan Ford. Workshop on Privacy in the Electronic Society (WPES), October 2016.
41. *PriFi: A Low-Latency and Tracking-Resistant Protocol for Local-Area Anonymous Communication*, Ludovic Barman, Mahdi Zamani, Italo Dacosta, Joan Feigenbaum, Bryan Ford, Jean-Pierre Hubaux, David Wolinsky. Workshop on Privacy in the Electronic Society (WPES), October 2016.
42. *Managing Identities Using Blockchains and CoSi*, Eleftherios Kokoris-Kogias, Linus Gasser, Ismail Khoffi, Philipp Jovanovic, Nicolas Gailly, Bryan Ford. 9th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs), July 2016.

43. *Certificate Cothority: Towards Trustworthy Collective CAs*, Ewa Syta, Iulia Tamas, Dylan Visher, David Isaac Wolinsky, and Bryan Ford. 8th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs), July 2015.

44. *Catching Bandits and* Only *Bandits: Privacy-Preserving Intersection Warrants for Lawful Surveillance*, Aaron Segal, Bryan Ford, and Joan Feigenbaum. 4th USENIX Workshop on Free and Open Communications on the Internet (FOCI), August 2014.

45. *From Onions to Shallots: Rewarding Tor Relays with TEARS*, Rob Jansen, Andrew Miller, Paul Syverson, and Bryan Ford. 7th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs), July 2014.

46. *A TorPath to TorCoin: Proof-of-Bandwidth Altcoins for Compensating Relays*, Mainak Ghosh, Miles Richardson, and Bryan Ford. 7th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs), July 2014.

47. *Crypto-Book: An Architecture for Privacy Preserving Online Identities*, John Maheswaran, David Isaac Wolinsky, and Bryan Ford. Twelfth ACM Workshop on Hot Topics in Networks (HotNets), November 2013.

48. *Conscript Your Friends into Larger Anonymity Sets with JavaScript*, Henry Corrigan-Gibbs and Bryan Ford. Workshop on Privacy in the Electronic Society (WPES), November 2013.

49. *Structural Cloud Audits that Protect Private Information*, Hongda Xiao, Bryan Ford, and Joan Feigenbaum. ACM Cloud Computing Security Workshop (CCSW), November 2013.

50. *An Untold Story of Redundant Clouds: Making Your Service Deployment Truly Reliable*, Ennan Zhai, Ruichuan Chen, David Isaac Wolinsky, and Bryan Ford. 9th Workshop on Hot Topics in Dependable Systems (HotDep), November 2013.

51. *Reducing Latency in Tor Circuits with Unordered Delivery*, Michael F. Nowlan, David Isaac Wolinsky, and Bryan Ford. 3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI), August 2013.

52. *Lazy Tree Mapping: Generalizing and Scaling Deterministic Parallelism*, Yu Zhang and Bryan Ford. 4th Asia-Pacific Workshop on Systems (APSYS), July 2013.

53. *Welcome to the World of Human Rights: Please Make Yourself Uncomfortable*, Henry Corrigan-Gibbs and Bryan Ford. Cyber-security Research Ethics Dialog & Strategy Workshop (CREDS), May 2013.

54. *Scavenging for Anonymity with BlogDrop*, Henry Corrigan-Gibbs and Bryan Ford. Provable Privacy Workshop (ProvPriv), July 2012.

55. *Icebergs in the Clouds: the Other Risks of Cloud Computing*, Bryan Ford. 4th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud), June 2012.

56. *Plugging Side-Channel Leaks with Timing Information Flow Control*, Bryan Ford. 4th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud), June 2012.

57. *Non-Linear Compression: Gzip Me Not!*, Michael F. Nowlan and Bryan Ford. 4th USENIX Workshop on Hot Topics in Storage and File Systems (HotStorage), June 2012.

58. *Scalable Anonymous Group Communication in the Anytrust Model*, David Isaac Wolinsky, Henry Corrigan-Gibbs, Bryan Ford, and Aaron Johnson. 5th European Workshop on Systems Security (EuroSec), April 2012.

59. *Faceless: decentralized anonymous group messaging for online social networks*, Xiaoxiao Song, David Isaac Wolinsky, and Bryan Ford. 5th Workshop on Social Network Systems (SNS), April 2012.

60. *A Virtual Memory Foundation for Scalable Deterministic Parallelism*, Yu Zhang and Bryan Ford. 2nd ACM SIGOPS Asia-Pacific Workshop on Systems (APSys), July 2011.

61. *CertiKOS: A Certified Kernel for Secure Cloud Computing*, Liang Gu, Alexander Vaynberg, Bryan Ford, Zhong Shao, and David Costanzo. 2nd ACM SIGOPS Asia-Pacific Workshop on Systems (APSys), July 2011.

62. *Deterministic OpenMP for Race-Free Parallelism*, Amittai Aviram and Bryan Ford. 3rd USENIX Workshop on Hot Topics in Parallelism (HotPar), May 2011.
63. *Workspace Consistency: A Programming Model for Shared Memory Parallelism*, Amittai Aviram, Bryan Ford, and Yu Zhang. 2nd Workshop on Determinism and Correctness in Parallel Programming (WoDet), March 2011.
64. *Minion—an All-Terrain Packet Packhorse to Jump-Start Stalled Internet Transports*, Janardhan Iyengar, Bryan Ford, Dishant Ailawadi, Syed Obaid Amin, Michael Nowlan, Nabin Tiwari, and Jeff Wise. 8th International Workshop on Protocols for Future, Large-Scale & Diverse Network Transports (PFLDNeT), November 2010.
65. *Determinating Timing Channels in Compute Clouds*, Amittai Aviram, Sen Hu, Bryan Ford, and Ramakrishna Gummadi. ACM Cloud Computing Security Workshop (CCSW), October 2010.
66. *An Efficient Cross-Layer Negotiation Protocol*, Bryan Ford and Janardhan Iyengar. 8th Workshop on Hot Topics in Networks (HotNets), October 2009.
67. *Device Transparency: a New Model for Mobile Storage*, Jacob Strauss, Chris Lesniewski-Laas, Justin Mazzola Paluska, Bryan Ford, Robert Morris, and Frans Kaashoek. SOSP Workshop on Hot Topics in Storage and File Systems (HotStorage), October 2009.
68. *Breaking Up the Transport Logjam*, Bryan Ford and Janardhan Iyengar. 7th Workshop on Hot Topics in Networks (HotNets), October 2008.
69. *An Offline Foundation for Online Accountable Pseudonyms*, Bryan Ford and Jacob Strauss. First International Workshop on Social Network Systems, April 2008.
70. *User-Relative Names for Globally Connected Personal Devices*, Bryan Ford, Jacob Strauss, Chris Lesniewski-Laas, Sean Rhea, Frans Kaashoek, and Robert Morris. 5th International Workshop on Peer-to-Peer Systems (IPTPS), February 2006.
71. *Unmanaged Internet Protocol: Taming the Edge Network Management Crisis*, Bryan Ford. 2nd Workshop on Hot Topics in Networks (HotNets), November 2003.
72. *The Flux OS Toolkit: Reusable Components for OS Implementation*, Bryan Ford, Jay Lepreau, Steve Clawson, Kevin Van Maren, Bart Robinson, and Jeff Turner. 6th IEEE Workshop on Hot Topics in Operating Systems (HotOS), May 1997.
73. *User-level Checkpointing through Exportable Kernel State*, Patrick Tullmann, Jay Lepreau, Bryan Ford, and Mike Hibler. 5th IEEE International Workshop on Object-Orientation in Operating Systems (IWOOOS), October 1996.
74. *The Persistent Relevance of the Local Operating System to Global Applications*, Jay Lepreau, Bryan Ford, and Mike Hibler. 7th ACM SIGOPS European Workshop, September 1996.
75. *Microkernels Should Support Passive Objects*, Bryan Ford and Jay Lepreau. 3rd IEEE International Workshop on Object-Orientation in Operating Systems (IWOOOS), December 1993.
76. *FLEX: A Tool for Building Efficient and Flexible Systems*, John B. Carter, Bryan Ford, Mike Hibler, Ravindra Kuramkote, Jeffrey Law, Jay Lepreau, Douglas B. Orr, Leigh Stoller, and Mark Swanson. 4th Workshop on Workstation Operating Systems (WWOS), October 1993.

Internet RFCs

77. *Unintended Consequences of NAT Deployments with Overlapping Address Space*, P. Srisuresh and B. Ford. RFC 5684, February 2010.
78. *NAT Behavioral Requirements for ICMP*, P. Srisuresh, B. Ford, S. Sivakumar, S. Guha. RFC 5508, April 2009.
79. *NAT Behavioral Requirements for TCP*, S. Guha, K. Biswas, B. Ford, S. Sivakumar, and P. Srisuresh. RFC 5382, October 2008.
80. *State of Peer-to-Peer (P2P) Communication across Network Address Translators (NATs)*, Pyda Srisuresh, Bryan Ford, and Dan Kegel. RFC 5128, March 2008.

Technical Reports and Other Publications

81. *Scaling Software-Defined Network Controllers on Multicore Servers*, Andreas Voellmy, Bryan Ford, Paul Hudak, and Y. Richard Yang. Yale University Technical Report TR1468, July 2012.
82. *Strong Theft-Proof Privacy-Preserving Biometric Authentication*, Ewa Syta, Michael J. Fischer, Abraham Silberschatz, Gina Gallegos Garca, and Bryan Ford. Yale University Technical Report TR1455, May 25, 2012.
83. *Advanced Development of Certified OS Kernels*, Zhong Shao and Bryan Ford. Yale University Technical Report TR1436, July 15, 2010.
84. *UIA: A Global Connectivity Architecture for Mobile Personal Devices*, Bryan Ford. Ph.D. thesis, Massachusetts Institute of Technology, September 2008. Supervisor: Professor Frans Kaashoek
85. *Directions in Internet Transport Evolution*, Bryan Ford. IETF Journal, Volume 3 Issue 3, December 2007.
86. *Scalable Internet Routing on Topology-Independent Node Identities*, Bryan Ford. Technical Report MIT-LCS-TR-926, October 31, 2003.
87. *Packrat Parsing: a Practical Linear-Time Algorithm with Backtracking*, Bryan Ford. Master's thesis, Massachusetts Institute of Technology, September 2002. Supervisor: Professor Frans Kaashoek
88. *Using Annotated Interface Definitions to Optimize RPC*, Bryan Ford, Mike Hibler, and Jay Lepreau. Technical Report UUCS-95-014, March 1995.
89. *Separating Presentation from Interface in RPC and IDLs*, Bryan Ford, Mike Hibler, and Jay Lepreau. Technical Report UUCS-95-018, December 1994.
90. *Notes on Thread Models in Mach 3.0*, Bryan Ford, Mike Hibler, and Jay Lepreau. Technical Report UUCS-93-012, April 1993.

Broader Audience Publications

91. *Seeking Anonymity in an Internet Panopticon*, Joan Feigenbaum and Bryan Ford. *Communications of the ACM*, 58(10), October 2015.
92. *GPUfs: the case for operating system services on GPUs*, Mark Silberstein, Bryan Ford, and Emmett Witchel. *Communications of the ACM*, 57(12), December 2014.
93. *Technology Can Make Lawful Surveillance Both Open and Effective*, Bryan Ford and Joan Feigenbaum. MIT Technology Review, August 18, 2014.
94. *Is Data Hoarding Necessary for Lawful Surveillance?* Bryan Ford and Joan Feigenbaum. Huffington Post, April 19, 2014.
95. *An Open Letter from US Researchers in Cryptography and Information Security.* January 24, 2014.
96. *Efficient System-Enforced Deterministic Parallelism (Research Highlights)*, Amittai Aviram, Shu-Chun Weng, Sen Hu, and Bryan Ford. *Communications of the ACM* 55(5), May 2012.

Coverage in Popular Media

Building a new Tor that can resist next-generation state surveillance, J.M. Porup, arstechnica, August 31, 2016.

On Riffle: An Efficient Communication System With Strong Anonymity:

- Riffle is Tor's spiritual successor for next-gen anonymous networks, TelecomsTech, Ryan Daws, July 13, 2016.
- Meet Riffle, the next-gen anonymity network that hopes to trounce Tor, The Register, Iain Thomson, July 13, 2016.
- MIT Anonymity Network Riffle Promises Efficiency, Security, ThreatPost, Chris Brook, July 13, 2016.
- Riffle, le rseau anonyme qui veut supplanter Tor, 20 minutes, July 12, 2016.

- Riffle Is More Secure, and Less Useful, Than Tor, Inverse, Nathaniel Mott, July 12, 2016.
- Riffle is a new anonymous sharing technique 10 times faster than predecessors, the Inquirer, Chris Merriman, July 12, 2016.
- MIT Thinks It Can One-Up TOR With New Anonymity Network: Riffle, Hackaday, Mike Szczys, July 12, 2016.
- Riffle a new anonymity network by MIT is more secure than Tor, TechWorm, Kavita Iyer, July 12, 2016.
- MIT communication platform Riffle could surpass Tor in anonymity, International Business Times, India Ashok, July 12, 2016.
- MITs Riffle is an anonymous network more secure than Tor, Firstpost, Aditya Madanapalle, July 12, 2016.
- MIT: Our Anonymity Network Riffle Is Better than Tor, Softpedia, Catalin Cimpanu, July 12, 2016.
- Researchers are developing an anonymity network more secure than Tor, dna India, July 12, 2016.
- New secure communication system plugs Tors vulnerabilities, Engineering and Technology Magazine, Tereza Pultarova, July 12, 2016.
- MIT's New Anonymity Network Is Claimed to Be More Secure Than Tor, Gadgets360, Shekhar Thakran, July 12, 2016.
- After Tor exploit, researchers develop new anonymity network, SC Magazine, Jeremy Seth Davis, July 12, 2016.
- How To Stay Anonymous Online? Researchers At MITs Computer Science And Artificial Intelligence Laboratory Are Working On A New Anonymity Scheme!, University Herald, Vinay Patel, July 12, 2016.
- MITs anonymous online communications protocol Riffle could beat Tor at its own game, TechCrunch, Devin Coldewey, July 11, 2016.
- MIT anonymity network promises to be more secure than Tor, engadget, Jon Fingas, July 11, 2016.
- MIT Researchers Devise New Anonymity Network Following Tor Bug, PC Magazine, Angela Moscaritolo, July 11, 2016.
- Researchers tout new anonymity network, The Hill, Joe Uchill, July 11, 2016.
- MIT Researchers Create Secure, Fast Anonymity System, Campus Technology, Sri Ravipati, July 11, 2016.
- How to stay anonymous online, MIT News, July 11, 2016.

On Apple, FBI, and Software Transparency:

- Guest on *Justice Radio with Steven Rambam*, March 23, 2016.
- Guest on *Loud & Clear with Brian Becker*, March 22, 2016.
- *How Apple Could Fed-Proof Its Software Update System*, MIT Technology Review, Tom Simonite, March 11, 2016.
- *Apple fears gov't overreach, Cothority offers co. help*, SC Magazine, Teri Robinson, March 10, 2016.
- *Cothority offers to help Apple security with distributed cosigning*, MacNN, March 10, 2016.
- *Using distributed code-signatures to make it much harder to order secret backdoors*, BoingBoing, Cory Doctorow, March 10, 2016.
- *Cothority to Apple: Lets make secret backdoors impossible*, arstechnica UK, J.M. Porup, March 10, 2016.

Dragons and butterflies: The chaos of other people's clouds, The Register, Danny Bradbury, February 5, 2016.

Co-thority statt Authority: Viele-Augen-Prinzip für Zertifikate, Heise (Germany), Monika Ermert, November 5, 2015.

'Dissent,' a New Type of Security Tool, Could Markedly Improve Online Anonymity, Motherboard, J.M. Porup, September 16, 2015.

Inside Cyber Security: Experts Talk Tech, WPNR News program "Where We Live" with John Dankosky, January 13, 2015.

On ***mass surveillance***:

- *Yale profs propose openness, crypto for disciplined surveillance*, John Fontana. ZDNet, August 20, 2014.
- *Researchers say you can surveil everyone and see only the criminals*, Zach Wener-Fligner. Quartz, August 20, 2014.
- *Some of the biggest names in cryptography condemn NSA spying in open letter*, Andrea Peterson, January 24, 2014.
- *US crypto researchers to NSA: If you must track, track responsibly*, Nidhi Subbaraman, NBC News, January 27, 2014.

On ***The Dissent Project***:

- *Privacy, please: New technologies could hide your identity online*, Nidhi Subbaraman, NBC News, June 14, 2013.

Icebergs in the Clouds [HotCloud '12] covered by many journalists and tech bloggers including:

- *Detailed Questions Hit the Cloud*, Greg Goth, IEEE Internet Computing, Sep-Oct, 2012.
- *That Glorious Fireworks Fail Last Week? Imagine That's Your Data*, Edward Tenner, The Atlantic, July 13, 2012.
- *Amazon Web Services: The hidden bugs that made AWS' outage worse*, Jack Clark, Cloud Watch, July 3, 2012.
- *The Cloud, or a Monster on the Loose?*, Arthur Cole, ITBusinessEdge, June 11, 2012.
- *Cloudburst: Unexplored Risks of the Cloud*, Keith Dawson, Business Agility, April 4, 2012.
- *The Risk of a Meltdown In the Cloud*, Slashdot, March 20, 2012.

On ***Determinating Timing Channels in Compute Clouds*** paper [CCSW '10]:

- *Spotting Virtual Intruders*, Erica Naone, MIT Technology Review, March 9, 2011.

Industry Experience

Nuvoiz Inc. — Mountain View, CA
Consultant — 2006
Provided design assistance on NAT traversal technology for voice-over-IP communication.

Phobos Inc. (acquired by SonicWALL in 2000) — Salt Lake City, UT
Systems architect — 1998–2000
Designed high-speed traffic management hardware/software systems in a networking startup.

Sleepless Software — Salt Lake City, UT
Founder — 1993–1998
Developed and marketed entertainment products for MS-DOS, Windows, and Java platforms.

Open Software Foundation — Cambridge, MA
Consultant — 1993
Advised on integration of fast RPC and migrating threads into the OSF Mach kernel.

Hewlett-Packard — McMinnville, OR
Software engineer — summer 1992
Cardiology Business Unit: wrote database tools for an ECG management system.

Designing Minds — Logan, UT
Consultant — 1991–1992
Designed and wrote drivers for high-speed data compression hardware.

Waterford Institute — Provo, UT
Software engineer — summers 1989–1991
Created educational curricula and software with a team of teachers and programmers,

Designing Minds — Logan, UT
Consultant — 1987–1988
Developed a painting program for bitmapped graphics and animation on the Amiga, titled *Chroma Paint*, published 1988.

Software Artifacts Publicly Released

2015 Cothority: scalable collective authority prototype.

2012 Dissent: an accountable anonymous group communication system. Open source release.

2010 Determinator/PIOS: an experimental research/instructional operating system. Open source release.

2007 SST: an experimental transport protocol implemented as a C++ library. Open source release.

2005 UIA: a naming and routing protocol suite for personal mobile devices. Open source release.

2005 vx32: an application-level virtual machine/sandbox for x86. Open source release.

2002 Pappy: a packrat parser generator for Haskell. Open source release.

1999 Fluke: an experimental microkernel operating system. Open source release.

1998 Flux OSKit: a component library for operating system construction. Open source release.

1997 Flick: an optimizing Interface Definition Language (IDL) compiler. Open source release.

1995 Inner Worlds: a side-scrolling action/adventure game. Released as Shareware by Sleepless Software.

1993 Migrating Threads: an enhancement to Mach 3.0, later incorporated in OSF Mach and Mac OS X.

1989 MultiPlayer: a multi-format music player for Amiga computers. Released as Shareware by author.

1988 Chroma Paint: a bitmapped graphics tool for Amiga. Commercially published by Designing Minds.