Brad Karp

Department of Computer Science
University College London
Gower Street
London, WC1E 6BT
United Kingdom

+44 20 7679 0406
`http://www.cs.ucl.ac.uk/staff/B.Karp/`
`bkarp@cs.ucl.ac.uk`

Education

Harvard University, Cambridge, MA, USA.
Doctor of Philosophy in Computer Science, November 2000.
Thesis title: *Geographic Routing for Wireless Networks.*
Master of Science in Computer Science, June 1995.
Advisor: H. T. Kung.

Yale University, New Haven, CT, USA.
Bachelor of Science in Computer Science, May 1992.
Thesis title: *Massively Parallel Algorithms for Adaptive Function Approximation in One and Two Dimensions.*

Professional History

Professor of Computer Systems and Networks, University College London, Department of Computer Science, London, UK: October 2014–present. Head of Systems and Networks Research Group (September 2010–present). Lead PhD students and Masters students in computer systems security and networking research; teach graduate and undergraduate classes in networking, distributed systems, and systems security.

Reader in Computer Systems and Networks, University College London, Department of Computer Science, London, UK: October 2007–September 2014. Same research and teaching responsibilities as present position.

Senior Lecturer, University College London, Department of Computer Science, London, UK: October 2005–September 2007. Same research and teaching responsibilities as present position.

Adjunct Assistant Professor, Carnegie Mellon University, Computer Science Department, Pittsburgh, PA, USA: September 2002–September 2005. Co-taught graduate courses in networking; co-advised two CMU PhD students on network security research.

Senior Staff Researcher, Intel Research Pittsburgh, Pittsburgh, PA, USA: September 2002–September 2005. Framed and led the Autograph and Polygraph worm signature generation projects. Framed and co-led the Open DHT distributed systems project. Led research on geographic routing, sensor networks, and other networked systems topics. Advised PhD student interns from UC Berkeley, CMU, and Princeton. Designed and ran PhD intern selection process for the lab.

Research Scientist, ICSI Center for Internet Research, University of California at Berkeley, Berkeley, CA, USA: October 2000–October 2002. Developed algorithms for improving TCP's robustness to packet reordering, techniques for geographic provisioning of wireless networks, and GHT, a distributed storage system for sensor networks, built on GPSR.

Research Intern, AT&T Center for Internet Research at ICSI, University of California at Berkeley, Berkeley, CA, USA: June 1999–April 2000. Developed GPSR, a scalable geographic routing system for wireless networks.

Research Intern, Digital Equipment Corporation, Littleton, MA, USA: June 1996–August 1996. Designed, simulated, and evaluated open-loop and best-effort traffic scheduling algorithms for input-buffered switch architectures.

Research Assistant, USC/Information Sciences Institute, Arlington, VA, USA: June 1995–August 1995. Designed and built a software-based ATM Forum ABR/EPRCA system for PC hardware with an experimental Intel ATM interface, running UNIX.

Board Memberships

Member, Board of Trustees, International Computer Science Institute (ICSI), University of California, Berkeley: 2017–present.

Peer Review Service

Steering Committee Memberships:
ACM SIGCOMM Conference (term 2016–2018; **chair 2017**).
ACM HotNets Workshop (term 2010–2014).

Program Committee Memberships:
ACM SOSP Conference: 2019, 2017, 2015.
ACM HotOS Workshop: 2019.
ACM ASPLOS Conference: 2019.
ACM HotNets Workshop: 2017 (**PC co-chair**), 2008.
IEEE Security and Privacy ("Oakland") Conference: 2017.
ACM SIGCOMM Conference: 2016, 2015 (**PC co-chair**, 2014, 2013, 2012, 2011, 2009, 2006.
USENIX/ACM NSDI Conference: 2016, 2013, 2012, 2011, 2008, 2007.
ACM EuroSys Conference: 2013.
USENIX/ACM OSDI Conference: 2010.
IEEE/ACM MobiCom Conference: 2008, 2005, 2004.
ACM SenSys Conference: 2007.
IEEE IPSN Conference: 2010, 2006.
IPTPS Workshop: 2006.
ACM/USENIX WORLDS Workshop (affiliated with OSDI): 2005 **(PC co-chair)**, 2004.
IEEE INFOCOM Conference: 2005.
IEEE NET+DB Workshop (affiliated with ICDE): 2005.
IEEE RTSS Conference (Sensor Networks Track): 2003.
ACM WSNA Workshop (affiliated with MobiCom): 2003.

Peer Review for Major Prizes:
IEEE Internet Award Committee (term 2015-2018).

Peer Review for Funding Agencies:
UK EPSRC: 2009-2017. Reviewer for proposals on networking and security research. Panelist to determine funding allocations across breadth of Computer Science.
EU ERC: 2011-2016. Reviewer for ERC proposals (starting, consolidator, and advanced) on networking and security research.
US NSF: 2007, 2004. Review panelist for proposals in the areas of computer networking, distributed systems, and systems security.

Prizes, Awards, and Other Honors

Departmental Teaching Award (2018) for excellence in teaching UCL CS 3007, Computer Systems.

Distinguished Reviewer Award (2017) for excellence in peer review for IEEE S&P ("Oakland") 2017.

Best Paper Award (2014) for HACK: Hierarchical ACKs for Efficient Wireless Medium Utilization, in *USENIX ATC 2014.*

Royal Society-Wolfson Research Merit Award (2005) for excellence in research, awarded to recruit leading academics in the sciences to UK universities.

Henry Dunster Tutor Prize (1997) for excellence in advising Harvard undergraduates.

Best Student Paper Award (1994) for Secure Short-Cut Routing for Mobile IP in *USENIX 1994*.

Research Interests

Computer systems, networks, and their algorithms. Main thrusts in computer system and network security (secure web browser architecture, exploit-resistant software, secure operating system primitives, Internet worm quarantine), wireless and Internet networking (routing, capacity), and large-scale distributed systems (distributed storage and rendezvous systems).

Ongoing Research Activity

Privacy-Preserving Cloud Computing: 2016-present. The modern era of *cloud computing* has made it cheaper and easier to deploy Internet-accessible services, but at a material cost in users' security and privacy. A company that wishes to provide a service to users—whether document sharing (in the style of Dropbox), calendaring, document translation, *etc.*—can simply deploy its servers as tenant VMs with a cloud provider. Cloud-based services tend to cryptographically protect the confidentiality and integrity of users' sensitive information crossing the Internet with SSL/TLS. SSL/TLS in turn places a private key on the server, the possession of which is sufficient to prove to clients that the server is the true server. It is here that cloud computing presents a grave security and privacy concern: because the cloud provider (*e.g.,* Amazon) can today see everything inside its tenants' VMs, Amazon (and its system administrator employees) can read a tenant service's SSL/TLS private key, and thus can create a rogue server that impersonates that service unbeknownst to the user. By leveraging new SGX Intel CPU hardware, which allows the encryption of code and data in an *enclave* memory region, we are designing and building an SSL/TLS web server that runs as a tenant service in the cloud *while keeping the server's SSL/TLS private key entirely secret from the cloud service provider.* The resulting web server denies the cloud provider access to its SSL/TLS private key. Indeed, not even an exploit of any of the millions of lines of application, OS, and hypervisor code running outside the secure enclave can compromise the tenant server's SSL/TLS private key.

COWL: Strong Privacy for Web-Based Applications: 2013–present. The web browser has become an attractive target for attackers who wish to obtain users' sensitive data. The browser's execution environment is complex: pages execute scripts, often from untrusted parties. We are designing and building COWL, a general-purpose information flow control (IFC) mechanism for JavaScript in web browsers, at a browser-frame granularity. COWL provides robust confinement for all JavaScript, and thus prevents malicious third-party scripts from leaking a user's sensitive information, enables flexible mashup web applications that cannot compromise a user's privacy, and allows browser extensions to become *untrusted* code. This work is in collaboration with Google, the Mozilla Foundation, and Stanford University.

Cooperative Power Allocation (COPA) and Cone of Silence (CoS): 2009–2015. Led two UCL PhD students in the development of algorithms and systems that leverage phased array antennas to improve capacity in 802.11 wireless networks. As 802.11 wireless networks proliferate, especially in densely populated urban areas, adjacent networks compete for finite capacity, and interference reduces throughput. When a sender of interest and other interferers transmit concurrently in a wireless network, CoS adaptively *nulls* interference to allow successful reception of the intended sender's signal. CoS permits an 802.11 access point to reduce the interference it generates in neighboring networks when transmitting to its own client, provided that doing so does not reduce throughput at its own client. COPA allows two neighboring APs to *cooperatively* null toward one another's clients, each taking account of the four MIMO wireless channels among the two APs and the two of their clients to which the APs concurrently transmit.

Past Research Activity

Efficient Feedback for High-Throughput Wireless Networks: 2012–2014. Today's fastest 802.11n wireless LANs offer physical-layer data rates up to 600 Mbps. At these rates, today's medium access control (MAC) protocols significantly limit achievable end-to-end throughput. And future, higher-rate wireless LANs will suffer even more from the same MAC protocol performance limitations. 802.11n's frame aggregation attempts to improve the MAC protocol's efficiency by sending multiple frames per medium acquisition. But TCP's acknowledgements still incur unnecessary medium access delays. In this work, we contribute TCP-BLACK (TCP with Block Link-layer ACKnowledgements), a cross-layer optimization that improves TCP throughput over 802.11n and future high-throughput wireless networks. TCP BLACK incorporates TCP acknowledgements into the link-layer ACKs sent by wireless receivers. On receiving TCP ACK information embedded in a link-layer ACK, an AP generates and forwards the corresponding TCP ACK on behalf of the receiver. By eliminating medium acquisitions for TCP ACK transmissions on the wireless channel, TCP BLACK can improve throughput by more than 20% as compared with 802.11n with perfect frame aggregation. We are demonstrating this scheme's practical feasibility with measurements of a prototype implementation for the SoRa software-defined radio platform.

Loop-Free Route Dissemination for a More Robust Internet: 2011–2013 (with collaborator Mark Handley). Today's Internet suffers from bouts of temporary unreachability that are a serious impediment to the robustness of real-time communication (such as Skype calls). Past measurement research has revealed that such unreachability largely occurs because of temporary loops and black holes in routing introduced by BGP, the Internet's wide-area routing protocol. In this work, we consider the intra-domain route dissemination problem from first principles, and show that these pathologies are not fundamental—rather, they are artifacts of iBGP, the protocol used for intra-domain route dissemination in today's Internet. We propose the Link-Ordered Update Protocol (LOUP), a clean-slate dissemination protocol for external routes that does not create transient loops, makes stable route choices in the presence of failures, and achieves policy-compliant routing without requiring any configuration. To illustrate the practicality of LOUP in deployment, we are building an implementation of the protocol for the Quagga open-source IP router, which we will release open-source.

Exploit-Resistant Protocol Implementations: 2009–2013. Led a UCL PhD student in developing architectural principles to protect sensitive data in software implementations of cryptographic protocols despite exploits. Discovered two novel classes of attack on state-of-the-art servers (including OpenSSH and the DStar DIFC SSL web server)—session key disclosure attacks and oracle attacks—that allow disclosure of users' sensitive data. Proposed fundamental architectural principles for cryptographic protocol implementations that thwart these attacks, and implemented them for the OpenSSH client and server and the OpenSSL library, the latter transparently hardening the cryptographic protocols used by a wide array of modern networked applications.

Wedge: 2007–2009. Led two UCL PhD students in developing novel operating system primitives and software development tools to protect sensitive data in network server software despite exploits. The Wedge OS primitives allow the creation of default-deny processes that inherit no data from a parent by default, compelling the programmer to explicitly enumerate code's privileges, and thus enabling strict adherence to the principle of least privilege. To ease the fine-grained privilege-separation of complex, monolithic legacy code, Wedge includes crowbar, a set of tools that use dynamic analysis to analyze memory allocation and access behavior, to help programmers determine exactly which minimal privileges to grant explicitly to which code in an application.

Autograph, Polygraph, and Paragraph: 2003–2006. Led two Carnegie Mellon Ph.D. students in the design and building of systems that automatically derive the signatures of novel Internet worms. A signature may be used to filter worm traffic, and thus halt a worm's spread. To do its work, **Autograph** analyzes traffic that crosses an edge network's DMZ in two steps: suspicious flow selection and content analysis. Autograph instances distributed at edge networks throughout the Internet share their observations; this information sharing significantly speeds Autograph's generation of signatures after a worm's initial release. An evaluation of Autograph on real DMZ traces from multiple sites reveals the system generates accurate signatures quickly: it would have generated a signature for the Code-RedI-v2 worm before 2% of vulnerable Internet hosts had become infected, without generating any signatures that cause false positives. **Polygraph** extends Autograph by generating signatures that can match even *polymorphic* worms, which vary their payload on every infection attempt in an effort to evade detection. Most recently, we describe **Paragraph**, a set of practical and effective attacks on the machine learning algorithms at the heart of worm signature generation systems and spam filters. The code for the Autograph and Polygraph systems runs on Linux and BSD hosts, and has been released open-source.

GPSR, CLDP, LCR, and applications: 1998–2007. Created and evaluated **Greedy Perimeter Stateless Routing (GPSR)**, a scalable routing algorithm for wireless and sensor networks that uses the *positions* of routers and a packet's destination to make forwarding decisions. In contrast, by using geography for forwarding decisions, GPSR requires state describing only a router's *immediate neighbor* routers. As a result, GPSR requires far less memory at each router—on the order of the number of a node's single-hop neighbors—than do previously proposed routing algorithms, which require storage on the order of the total number of nodes (DV) or links (LS) in the network. Because of this small state requirement, GPSR finds routes robustly after topology changes, and is highly message-efficient. With the **Crossing Link Detection Protocol (CLDP)**, we extend GPSR to be *provably correct* on *arbitrary connected network graphs, regardless of topology*. In the **Lazy Cross-link Removal protocol (LCR)**, we reduce the message complexity of geographic routing by two orders of magnitude, producing the most message-efficient geographic routing protocol known to date. Applications of geographic routing that rely on its unique scaling properties include **data-centric storage (DCS)** on sensor networks, through which sensors may store and answer queries over sensed data in an energy-efficient fashion, and **reduced-state routing (RSR)** for the Internet, through which forwarding table sizes at core routers may be drastically reduced.

Re: Reliable Email: 2005–2007. With collaborators from Stanford University, Carnegie Mellon University, and Intel Research, co-founded and co-led the Reliable Email (Re:) project, whose aim is to eliminate false positives caused during spam filtering, and thus to render email reliable between legitimate senders and recipients. Re: is a novel, distributed email whitelisting system that incurs zero false positives among socially connected users. Re: exploits *friend-of-friend* relationships among email correspondents to populate whitelists automatically. An evaluation using email traces from two large sites (one corporate and one academic) reveals that Re: can eliminate up to 88% of the false positives incurred by a widely deployed spam filtering system, at modest computational cost. Built a full prototype of Re:.

Open DHT: 2003–2006. As project co-PI, led two UC Berkeley Ph.D. students in designing, building, and deploying Open DHT, a publicly accessible distributed hash table (DHT) service. A DHT allows hosts distributed across the Internet to form an overlay network that provides a simple hash-table-like functionality, through which key-value pairs may be stored distributedly across those hosts. To spur adoption of DHTs and drive research on real systems built upon them, we have built and deployed Open DHT, a generic, reusable DHT service that is broadly useful as a building block for distributed applications. The system supports put and get operations on key-value pairs, and runs 24 hours per day, 7 days per week, on a collection of over 200 infrastructure hosts distributed across five continents. The system is public in that any Internet host may use it. Open DHT incorporates novel approaches to authenticating data in a distributed system shared by mutually distrusting users; to fair storage allocation for soft-state storage among Internet-scale client populations; and to supporting a shared routing layer among heterogeneous applications. It has found use in over 15 projects by researchers at institutions including MIT, UC Berkeley, HP Labs, UCL, Intel Research, and UCLA.

Reordering-Robust TCP: 2001–2003. With a student intern advisee, co-designed extensions to the TCP reliable transport protocol to improve its robustness on network paths that reorder packets. By relaxing today's constraint that the Internet must deliver packets in order, this work enables novel, previously untenable designs, such as flow-oblivious multi-path routing.

APRL and HUMR: 1997–1999. Designed and built a multi-hop wireless mobile network on commodity Metricom Ricochet radios. Created HUMR, an application-level UNIX driver for peer-to-peer IPv4 and IPv6 communication using Ricochet radios, that were ordinarily used only for PPP connections with Metricom's commercial wireless service. HUMR uses hints provided by the radios' firmware to detect acquisition and loss of neighbors. Created APRL, Any-Path Routing without Loops, a distance-vector routing system that *provably* does not acquire looping routes. Demonstrated the combined system running on mobile networks of dozens of hosts for the US Air Force.

SABRA: 1995–1996. Built SABRA, an ATM ABR with EPRCA rate-based flow control system for Intel hosts with a CMU/Harvard/Intel-designed ATM network interface and the Harvard/Nortel CreditNet ATM switch. Unlike previously proposed ABR implementations that required an ASIC on the host adapter, SABRA performs ABR in software on the host's CPU. SABRA can sustain the full OC-3 ATM link rate.

Mobile IP: 1993–1994. Collaborated in the design and building of the Harvard Mobile IP system, one of the first working Mobile IP implementations, when Mobile IP was still being defined. The Harvard system supports secure "short-cut" routing, through which wired hosts communicate directly with a roaming mobile host, rather than through the mobile host's home agent.

CreditNet: 1992–1995. As a member of a team comprised of H.T. Kung's lab at Harvard and a group at Nortel, co-designed the CreditNet switch, a multi-gigabit ATM switch with hardware support for per-circuit credit-based flow control. Built the first host-side N23 credit-based flow control system.

Publications

Refereed Articles

[1] Gvozdiev, N., Vissicchio, S., Karp, B., and Handley, M., On Low-Latency-Capable Topologies, and their Impact on the Design of Intra-Domain Routing, in the *Proceedings of the ACM SIGCOMM Conference on Computer Communications (SIGCOMM 2018)*, Budapest, Hungary, August 2018.

[2] Gvozdiev, N., Vissicchio, S., Karp, B., and Handley, M., Low-Latency Routing on Mesh-Like Backbones, in the *Proceedings of the Sixteenth ACM SIGCOMM Workshop on Hot Topics in Networks (HotNets 2017)*, Palo Alto, CA, November 2017.

[3] Nikolaidis, G., Handley, M., Jamieson, K., and Karp, B., COPA: Cooperative Power Allocation for Interfering Wireless Networks, in the *Proceedings of the Eleventh International Conference on Emerging Networking Experiments and Technologies (CoNEXT 2015)*, Heidelberg, Germany, December 2015.

[4] Gvozdiev, N., Karp, B., and Handley, M., FUBAR: Flow Utility-Based Routing, in the *Proceedings of the Thirteenth ACM SIGCOMM Workshop on Hot Topics in Networks (HotNets 2014),* Los Angeles, CA, October 2014.

[5] Yang, E., Stefan, D., Mitchell, J., Mazières, D., Marchenko, P., and Karp, B., Toward Principled Browser Security, in the *Proceedings of the Fourteenth Workshop on Hot Topics in Operating Systems (HotOS 2013),* Santa Ana Pueblo, NM, May 2013.

[6] Gvozdiev, N., Karp, B., and Handley, M., LOUP: The Principles and Practice of Intra-Domain Route Dissemination, in the *Proceedings of the Tenth USENIX Symposium on Networked Systems Design and Implementation (NSDI 2013),* Lombard, IL, April 2013.

[7] Gvozdiev, N., Karp, B. and Handley, M., LOUP: Who's Afraid of the Big Bad Loop?, in the *Proceedings of the Eleventh ACM SIGCOMM Workshop on Hot Topics in Networks (HotNets 2012),* Bellevue, WA, October 2012.

[8] Marchenko, P. and Karp, B., Structuring Protocol Implementations to Protect Sensitive Data, in the *Proceedings of the 19th USENIX Security Symposium (USENIX Security 2010)*, Washington, DC, August 2010.

[9] Bittau, A., Marchenko, P., Handley, M., and Karp, B., Wedge: Splitting Applications into Reduced-Privilege Compartments, in the *Proceedings of the Fifth USENIX/ACM Symposium on Networked System Design and Implementation (NSDI 2008)*, San Francisco, CA, April 2008.

[10] Kim, Y.-J., Govindan, R., Karp, B., and Shenker, S., Lazy Cross-Link Removal for Geographic Routing, in the *Proceedings of the Fourth ACM Conference on Embedded Network Sensor Systems (SenSys 2006),* November 2006.

[11] Newsome, J., Karp, B., and Song, D., Paragraph: Thwarting Signature Learning by Training Maliciously, in the *Proceedings of the Ninth International Symposium on Recent Advances in Intrusion Detection (RAID 2006),* September 2006.

[12] Garriss, S., Kaminsky, M., Freedman, M., Karp, B., Mazières, D., and Yu, H., Re: Reliable Email, in the *Proceedings of the Third USENIX/ACM Symposium on Networked System Design and Implementation (NSDI 2006),* May 2006.

[13] Kim, Y.-J., Govindan, R., Karp, B., and Shenker, S., On the Pitfalls of Geographic Face Routing, in the *Proceedings of the Third ACM/SIGMOBILE International Workshop on Foundations of Mobile Computer (DIAL-M-POMC 2005),* September 2005.

[14] Rhea, S., Godfrey, P.B., Karp, B., Kubiatowicz, J., Ratnasamy, S., and Shenker, S., Open DHT: A Public DHT Service and Its Uses, in the *Proceedings of the ACM SIGCOMM Conference on Computer Communications (SIGCOMM 2005),* August 2005.

[15] Newsome, J., Karp, B., and Song, D., Polygraph: Automatically Generating Signatures for Polymorphic Worms, in the *Proceedings of the IEEE Symposium on Security and Privacy (Oakland 2005),* May 2005.

[16] Kim, Y.-J., Govindan, R., Karp, B., and Shenker, S., Geographic Routing Made Practical, in the *Proceedings of the Second USENIX/ACM Symposium on Networked System Design and Implementation (NSDI 2005),* May 2005.

[17] Gummadi, R., Kothari, N., Kim, Y.-J., Govindan, R., Karp, B., and Shenker, S., Reduced State Routing in the Internet, in the *Proceedings of the Third ACM SIGCOMM Workshop on Hot Topics in Networks (HotNets 2004),* November 2004.

[18] Nath, S., Ke, Y., Gibbons, P., Karp, B., and Seshan, S., A Distributed Filtering Architecture for Multimedia Sensors, in *Proceedings of the First IEEE Workshop on Broadband Advanced Sensor Networks (BASENETS 2004),* October 2004.

[19] Kim, H.-A., and Karp, B., Autograph: Toward Automated, Distributed Worm Signature Generation, in *Proceedings of the 13th Annual USENIX Security Conference (USENIX Security 2004),* August 2004.

[20] Karp, B., Ratnasamy, S., Rhea, S., and Shenker, S., Spurring Adoption of DHTs with OpenHash, a Public DHT Service, in *Proceedings of the 3rd International Workshop on Peer-to-Peer Systems (IPTPS 2004),* Springer-Verlag Lecture Notes in Computer Science Hot Topics Series, February 2004.

[21] Gibbons, P., Karp, B., Nath, S., Ke, Y., and Seshan, S., IrisNet: An Architecture for a Worldwide Sensor Web, in *IEEE Pervasive Computing, Special Issue on Sensor and Actuator Networks,* IEEE Press, October–December 2003.

[22] Zhang, M., Karp, B., Floyd, S., and Peterson, L., RR-TCP: A Reordering-Robust TCP with DSACK, in *Proceedings of the 2003 IEEE International Conference on Network Protocols (ICNP 2003),* November 2003.
(Extended version published as ICSI Technical Report TR-02-006, July 2002.)

[23] Ratnasamy, S., Karp, B., Shenker, S., Estrin, D., Govindan, R., Yin, L., and Yu, F., Data-Centric Storage in Sensornets with GHT, A Geographic Hash Table, in *Mobile Networks and Applications (MONET)*, vol. 8, no. 4, Kluwer Academic Publishers, August 2003.

[24] Tolia, N., Kozuch, M., Satyanarayanan, M., Karp, B., Bressoud, T., and Perrig, A., Opportunistic Use of Content-Addressable Storage for Distributed File Systems, in the *Proceedings of the USENIX 2003 Technical Conference,* June 2003.

[25] Shenker, S., Ratnasamy, S., Karp, B., Govindan, R., and Estrin, D., Data-Centric Storage in Sensornets, in the *Proceedings of the First ACM SIGCOMM Workshop on Hot Topics in Networks (HotNets 2002),* October 2002.

[26] Ratnasamy, S., Karp, B., Yin, L., Yu, F., Estrin, D., Govindan, R., and Shenker, S., GHT: A Geographic Hash Table for Data-Centric Storage, in the *Proceedings of the First ACM International Workshop on Wireless Sensor Networks and Applications (WSNA 2002)*, September 2002.

[27] Karp, B. and Kung, H. T., Greedy Perimeter Stateless Routing for Wireless Networks, in *Proceedings of the Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 2000)*, August 2000, pp. 243–254.

[28] Gaynor, M., Karp, B., and Kung, H. T., A PC-Based ATM Link Delay Simulator, in *Proceedings of the 1998 Summer Computer Simulation Conference (SCSC '98)*, July 1998.

[29] Blackwell, T., Chan, K., Chang, K., Charuhas, T., Karp, B., Kung, H.T., Lin, D., Morris, R., Seltzer, M., Smith, M., Young, C., Bahgat, O., Chaar, M., Chapman, A., Depelteau, G., Grimble, K., Huang, S., Hung, P., Kemp, M., Mahna, I., McLaughlin, J., Ng, M.T., Vincent, J., Watchorn, J., An Experimental Flow-Controlled Multicast ATM Switch, in *Proceedings of the First Annual Conference on Telecommunications in Massachusetts*, October 1994.

[30] Blackwell, T., Chan, K., Chang, K., Charuhas, T., Gwertzman, J., Karp, B., Kung, H.T., Li, W.D., Lin, D., Morris, R., Polansky, R., Tang, D., Young, C., Zao, J., Secure Short-Cut Routing for Mobile IP, in *Conference Proceedings of the USENIX Summer 1994 Technical Conference*, Boston, Massachusetts, June 1994.

Other Publications

[31] Marchenko, P. and Karp, B., Protecting Sensitive Data in Web Browsers with ScriptPolice, UCL CS Research Note RN/13/02, January 2013, 13 pages.

[32] Nikolaidis, G., Zhushi, A., Jamieson, K., and Karp, B., Cone of Silence: Adaptively Nulling Interferers in Wireless Networks, UCL CS Research Note RN/10/02, January 2010, 14 pages.

[33] Karp, B., Mankin, A., Kung, H.T., Demirtjis, A., and Edwards, B., An Implementation Study of ABR/EPRCA, *ATM Forum Contribution 96-587*, April 1996.

[34] Karp, B. and Moulin, P., Implementation of Multiresolution Regression Splines on the MasPar: Function and Image Estimation in Parallel, *Bell Communications Research Internal Technical Memorandum*, February 1993.

[35] Karp, B. and Bischof, C., Increasing the Granularity of Parallelism and Reducing Contention in Automatic Differentiation, *Argonne National Laboratory Technical Memorandum ANL/MCS-TM-142*, November 1990.

Lectures

[36] Karp, B., Protecting Sensitive Data in Web Browsers with ScriptPolice, in the *Proceedings of the Thirteenth Annual High-Confidence Software and Systems Conference,* May 2013.

[37] Karp, B., Challenges in Geographic Routing: Sparse Networks, Obstacles, and Traffic Provisioning, in the *Proceedings of the DIMACS Workshop on Pervasive Networking*, May 2001.

Invited Talks ACM SYSTOR 2016, Safeguarding Users' Sensitive Data in the Cloud and Browser (Keynote Address), 8th June 2016.

Alan Turing Institute, Safeguarding Users' Sensitive Data in the Cloud and Browser (Turing Lecture in Computer Science, to inaugurate the Institute), 27th April 2016.

Microsoft Research, Practical Privacy for Web Users with COWL, 24th April 2015.

UCL, Protecting Users' Privacy in Modern Web Applications (Lunch Hour Lecture), 18th February 2015.

EPFL (Summer Research Institute), Protecting Sensitive Data in Web Browsers with ScriptPolice, 3rd June 2013.

ICSI, University of California at Berkeley (Colloquium), Protecting Sensitive Data in Networked Applications, 12th May 2011.

Cisco Systems (Tech Talk), Wedge: Protecting Sensitive Data in Complex Applications with Reduced-Privilege Compartments, 22nd October 2010.

EPFL (Summer Research Institute), Wedge: Splitting Complex, Monolithic Applications into Reduced-Privilege Compartments, 18th July 2008.

From Fundamentals to Infrastructure—Steps Towards the Future Internet (2nd CoNEXT Conference; COST-funded summit workshop between the EU ESF and US NSF on future funding directions for networked systems research), Networked Systems: Vulnerabilities and Adaptive Adversaries, 4th December 2006.

University of Southern California Computer Science Department (Colloquium), Evolution in Action: Worms and Worm Defenses, 9th November 2006.

US NSF (Workshop on Geometric Approaches to Ad Hoc and Sensor Networks), Respecting Reality in Sensor Network Algorithms (or 12 Steps to Giving Up the Unit-Disk Graph), 12th-13th June 2006.

Google Labs (Tech Talk), Re: Reliable Email, 11th May 2006.

Harvard University Computer Science Department (Colloquium), Evolution in Action: Worms and Worm Defenses, 2nd February 2006.

Intel Research (Security Summit Meeting), Generating Worm Signatures Automatically with Autograph and Polygraph, 18th November 2005.

Stanford University Computer Science Department (Networking Seminar), Generating Worm Signatures Automatically with Autograph and Polygraph, 10th November 2005.

Graduated Students

First Supervisor at UCL CS for PhD student Georgios Nikolaidis: receive and transmit nulling in wireless networks for capacity improvement; entered October 2008, graduated July 2016. Examiners: Srinivasan Seshan (CMU), Miguel Rio (UCL EE). First position: researcher at Barefoot Networks, Palo Alto, California.

First Supervisor at UCL CS for PhD student Petr Marchenko (ORS recipient): Stronger Secrecy for Network-Facing Applications through Privilege Reduction; entered January 2007, graduated August 2013. Examiners: Nickolai Zeldovich (MIT), Peter O'Hearn (UCL). First position: researcher in Google's Security Research Group, Mountain View, California.

Co-Supervisor (50%) at UCL CS for PhD student Andrea Bittau: securing commodity software; entered October 2005, completed November 2009. Examiners: Eddie Kohler (UCLA), Andrew Herbert (Microsoft Research Cambridge/UCL). First position: postdoc in David Mazières's Secure Computer Systems Group, Stanford University CS; then at Google's Security Research Group, Mountain View, California.

Second Supervisor at UCL CS for PhD student Lynne Salameh: multi-path transport for web page loads on multi-interface clients; entered October 2010, graduated April 2018.

Second Supervisor at UCL CS for PhD student Jie Xiong: angle-of-arrival measurement for wireless localization and authentication; entered January 2010, graduated September 2015. First position: assistant professor, Information Systesm Department, Singapore Management University, Singapore; now assistant professor, Computer Science Department, University of Massachusetts, Amherst.

Second Supervisor at UCL CS for PhD student Felipe Huici: DDoS defense; entered October 2004, graduated November 2009.

Thesis Committee Member at Carnegie Mellon University ECE for PhD student James Newsome: polymorphic worm signature generation and attacks on learning signature generation (primary supervisor of work that led to IEEE Oakland 2005 and RAID 2006 publications, significant results in his thesis), graduated October 2008. First position: researcher, Bosch Research, Pittsburgh.

Thesis Committee Member at Carnegie Mellon University CS for PhD student Hyang-Ah Kim: automated worm signature generation (sole supervisor of work that led to USENIX Security 2004 publication, the core of her thesis), graduated September 2007. First position: researcher, Google Labs New York.

Thesis Committee Member at University of Southern California CS for PhD student Young-Jin Kim: efficient and practical geographic routing (co-supervisor of work that led to NSDI 2005 and SenSys 2006 publications, both in my established area of geographic routing, and the core of his thesis), graduated December 2006. First position: researcher, Bell Labs.

First Supervisor at UCL CS for Masters thesis in Information Security (Katrina Joyce), awarded *distinction* in October 2013.

First Supervisor at UCL CS for Masters thesis in Information Security (Havard Sande), awarded *distinction* and best project in research area by UCL CS in October 2011.

First Supervisor at UCL CS for Masters thesis in Information Security (Petr Marchenko), awarded *distinction* in October 2006.

Current Students

First Supervisor at UCL CS for PhD student Ahmed Awad (ORS recipient): ensuring secrecy and integrity of tenant cloud computations; entered October 2017, expected completion September 2022.

Second Supervisor at UCL CS for PhD student Nikola Gvozdiev: delay-minimizing traffic engineering for ISP backbones and improved stability and robustness for BGP routing; entered October 2011, expected completion January 2019.

First Supervisor at UCL CS for PhD student Astrit Zhushi (ORS recipient): Cross-layer transport- and MAC-layer protocol design for efficient aggregation and bit-rate adaptation in WiFi networks; entered January 2011, expected completion January 2019.

Examining Activity

Internal Examiner (2013): Examined Stephanie Bayer for the PhD at UCL CS (first supervisor: Dr Jens Groth).

External Examiner (2010): Examined Periklis Akritidis for the PhD at the University of Cambridge Computing Laboratory (supervisor: Dr Steven Hand).

External Examiner (2007): Examined Pan Hui for the PhD at the University of Cambridge Computing Laboratory (supervisor: Professor Jon Crowcroft).

External Examiner (2006): Examined Eng Keong-Lua for the PhD at the University of Cambridge Computing Laboratory (supervisor: Dr Timothy Griffin).

Other Advising

Advisor (2004): Three Ph.D.-student research summer interns at Intel Research.

Advisor (2003): Two Ph.D.-student research summer interns at Intel Research.

Co-advisor (1998): Harvard University CS Bachelor's thesis (Michael Walfish), graded *summa cum laude* by Harvard's Computer Science Department.

Resident Tutor in Computer Science (1995–1999): Dunster House. Advised and assisted Harvard undergraduate Computer Science students in thesis topic selection, course work, problem sets, *&c.*

Teaching

Instructor (2018): Computer Systems (UCL CS 3007, undergraduate course): Taught all 30 lecture hours. Organized course, defined entire syllabus, designed programming courseworks.

Instructor (2007–2018): Distributed Systems and Security (UCL CS GZ03/M030, graduate course). Taught all 30 lecture hours. Organized course, defined entire syllabus, designed programming and problem set courseworks.

Co-instructor (2006–2016): Mobile and Cloud Computing (previously known as Mobile and Adaptive Systems) (UCL CS GZ06/M038, graduate course). Taught 15 (2006), 10 (2007–2010), 15 (2012–2015), and 30 (2016) of 30 total lecture hours. Organized course, defined full (2016), half (2006, 2012–2015) and one-third (2007–2010) of syllabus.

Co-instructor (2009–2014): Networked Systems (UCL CS GZ01/3035, graduate and undergraduate course). Taught 15 of 30 total lecture hours. Co-organized course, defined half syllabus, designed programming and problem set courseworks.

Co-instructor (2006-2009): Communications and Networks (UCL CS GC15/6007). Taught 15 of 30 total lecture hours. Organized course, defined entire syllabus, designed programming coursework.

Co-instructor (2003): Sensor Networks (Carnegie Mellon CS 15-829, graduate course). Taught 12 of 36 total lecture hours. Defined one-third of syllabus.

Co-instructor (1996): Operating System Network Performance (Harvard CS 248, graduate course). Taught 12 of 36 total lecture hours. Defined half of syllabus, designed programming coursework.

Teaching Fellow (1993): Operating Systems (Harvard CS 161/261, graduate and undergraduate course). Taught 12 one-hour sections to supplement instructor's lectures.

Consulting Activity

Expert Witness, Bristows, London, UK: February 2016–April 2016. Served as expert on behalf of Google against confidential counterparty in patent case in the UK High Court concerning mobile, wireless computing and cryptography. Prepared two reports; case ended before trial.

Expert Witness, Bristows, London, UK: March 2015–November 2015. Served as expert on behalf of MobileIron against counterparty Good Technology in patent case in the UK High Court concerning data synchronization for mobile devices. Prepared three reports; case ended before trial in settlement.

Expert Witness, Marks and Clerk, London, UK: June 2013–February 2015. Served as expert on behalf of Virgin Media against counterparty Rovi in patent case in the UK High Court concerning Internet (IP) packet forwarding and redirection. Prepared two reports; case ended before trial with Rovi's consenting to have their patent revoked in the UK.

Expert Witness, Freshfields, London, UK: December 2011–April 2012. Served as expert on behalf of Apple against counterparty HTC in patent case in the UK High Court concerning system software for mobile devices. Prepared three reports; testified in the witness box for one and a half days.

Expert Witness, Finnegan, Atlanta, GA, USA: January 2010–September 2010. Served as expert on behalf of Research in Motion (RIM, makers of the Blackberry) against counterparty Motorola in patent interference case before the USPTO concerning wireless networking systems. Prepared two declarations; completed two depositions. The USPTO judged in favor of RIM.

Expert Witness, Hogan Lovells and Allen and Overy, London, UK: July 2006–July 2009. Served as expert in three patent cases (two in the UK, one in the EPO) concerning networked computer systems (details confidential).

Due Diligence Consultant, Amadeus Capital Partners, London, UK: November 2007–January 2008. Served as technical expert to assess the ability of a networking startup company for investment from one of the largest and most selective venture capital firms in the UK. Work included a site visit to the startup, my interviewing the CEO, CTO, and senior technical staff, and my reviewing the designs of its network security and performance-enhancing hardware and software.

Visiting Faculty Consultant, Intel Research Cambridge, Cambridge, UK: October 2005–October 2007. Collaborated with researchers at Intel Research Cambridge on topics in 802.11 mesh networking.

Visiting Faculty Consultant, Intel Research Pittsburgh, Pittsburgh, PA, USA: October 2005–December 2007. Collaborated with researchers at Intel Research Pittsburgh, Stanford University, and Carnegie Mellon University on the design and evaluation of Re:, the social whitelisting system for email.

Collaborator, Hobnob, Pittsburgh, PA, USA: January 2005–October 2005. Fostered adoption of my Autograph worm signature generation system by computer security startup Hobnob, which deployed Autograph in-house, and rolled out Autograph deployments at its customers' sites in Q1 2006.

Professional Society Memberships

Member of ACM, USENIX.