

Bogdan Carbunar

CONTACT INFORMATION

Motorola Labs
E-mail: carbunar@gmail.com
Phone: (847) 241-2125
WWW: www.carbunar.com

EDUCATION

Purdue University, West Lafayette, Indiana, 1999-2005

Ph.D. in Computer Science, May 2005
Thesis: Coverage Problems in Wireless Sensor and RFID Systems
Advisor: Jan Vitek, Ananth Grama and Cristina Nita-Rotaru

“Politehnica” University, Bucharest, Romania, 1994-1999

B.S. in Computer Science, June 1999

RESEARCH EXPERIENCE

Principal Staff Research Engineer: Applications Research Center, Motorola Labs, 2005 - present.

- Design and development of collaborative caching algorithms for Video on Demand systems.
- Design and development of secure, periodic update synchronization methodologies for Wi-Fi enabled devices, intended to extend battery lifetime.
- Study and development of private information retrieval techniques. Design of new Oblivious RAM (ORAM) flavors: Write Once Read Many (WORM) semantics and access rights delegation.
- Design and development of Private Fuzzy Joins: allow data owners to privately run approximate match queries on data outsourced to untrusted servers.
- Experimental study of attacks on privacy in Facebook. Development of Facebook applications for capturing trust and blocking privacy leaks.
- Design of conditional e-cash tools and their application to micropayments for anonymous routing and secure computation outsourcing.

Doctoral Research: Department of Computer Sciences, Purdue University, 1999 - 2005 (research advisor: Dr. Jan Vitek, Dr. Ananth Grama, Dr. Cristina Nita-Rotaru).

- Propose novel coverage definitions for sensor networks and RFID systems. Find efficient, localized criteria and algorithms for determining and eliminating coverage redundancy in dense networks.
- Design and development of secure mechanisms for generating high throughput routes in hybrid cellular and ad hoc networks. Propose efficient algorithms for finding and maintaining quality routes, resilient to both selfish and purely malicious attacks.

RESEARCH INTERESTS

Applied cryptography, distributed system security and privacy with applications in:

- private data and computation outsourcing
- electronic payment technologies and their applications
- social networking privacy and security

PUBLICATIONS

BOOK AND BOOK CHAPTER

Bogdan Carbunar, Murali Krishna Ramanathan, Mehment Koyuturk, Suresh Jagannathan, Ananth Grama. Optimal Tag Coverage and Tag Report Elimination. To appear as book chapter in Wiley’s RFID Systems: Research Trends and Challenges, editors M. Bolic, D. Simplot-Ryl, I. Stojmenovic.

Bogdan Carbunar. Coverage Problems in Wireless Sensor and RFID Systems. VDM Verlag Dr. Muller. ISBN 978-3-639-12156-8.

JOURNALS

Bogdan Carbunar, Radu Sion. Write Once Read Many Oblivious RAM. To appear in the IEEE Transactions on Information Forensics and Security (TIFS).

Bogdan Carbunar, Radu Sion. Toward Private Joins on Outsourced Data. To appear in the IEEE Transactions on Knowledge and Data Engineering (TKDE).

Bogdan Carbunar, Mahesh Tripunitara. Payments for Outsourced Computations. To appear in the IEEE Transactions on Parallel and Distributed Systems (TPDS).

Bogdan Carbunar, Larry Shi, Radu Sion. Conditional E-Payments with Transferability. Journal of Parallel and Distributed Computing (JPDC), Volume 71, Issue 1, January 2011.

Bogdan Carbunar, Michael Pearce, Shivajit Mohapatra, Loren Rittle, Venu Vasudevan, Octavian Carbunar. Secure Synchronization of Periodic Updates in Ad Hoc Networks. IEEE Transactions on Parallel and Distributed Systems (TPDS), Volume 21, Number 8, 2010.

Bogdan Carbunar, Yang Yu, Weidong Shi, Michael Pearce, Venu Vasudevan. Query Privacy in wireless sensor networks. To appear in ACM Transactions on Sensor Networks (TOSN), Volume 6, Issue 2, 2010.

Bogdan Carbunar, Ioannis Ioannidis, Cristina Nita-Rotaru. JANUS: A Framework for Scalable and Secure Routing in Hybrid Wireless Networks. IEEE Transactions on Dependable and Secure Computing (TDSC), Volume 6, Number 4, 2009.

Siddharth Bhatt, Radu Sion, Bogdan Carbunar. A Personal Mobile DRM Manager for Smartphones. Elsevier Computers and Security Journal, Volume 28, Issue 6, September 2009.

Bogdan Carbunar, Murali Krishna Ramanathan, Mehmet Koyuturk, Suresh Jagannathan, Ananth Grama. Efficient Tag Detection in RFID Systems. Journal of Parallel and Distributed Computing (JPDC), Volume 69, Issue 2, 2009.

Bogdan Carbunar, Ananth Grama, Jan Vitek, Octavian Carbunar. Redundancy and Coverage Detection in Sensor Networks. ACM Transactions on Sensor Networks (TOSN), Volume 2, Issue 1, 2006.

Bogdan Carbunar, Marco Tulio Valente, Jan Vitek. Coordination and Mobility in CoreLime (extended version of the MA paper). Journal of Mathematical Structures in Computer Science 14(3), June 2004.

CONFERENCES

Bogdan Carbunar, Michael Pearce, Venu Vasudevan, Michael Needham. Predictive Caching for Video on Demand CDNs. To appear in the 54th IEEE Global Communications conference (GLOBECOM), Houston, December 2011.

Martin Franz, Bogdan Carbunar, Stefan Katzenbeisser, Radu Sion. Oblivious Outsourced Storage with Delegation. In Proceedings of the 15th International Conference on Financial Cryptography and Data Security (FC) [full paper acceptance rate=20%], St. Lucia, March 2011.

Bogdan Carbunar, Radu Sion. Regulatory Compliant Oblivious RAM. In Proceedings of the 8th International Conference on Applied Cryptography and Network Security (ACNS) [acceptance rate=18.5%], Beijing, June 2010.

Bogdan Carbunar, Mahesh Tripunitara. Fair Payments for Outsourced Computations. In Proceedings of the 7th IEEE International Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON) [acceptance rate=21%], Boston, June 2010.

Mahesh Tripunitara, Bogdan Carbunar. Efficient Access Enforcement in Distributed Role-Based Access Control (RBAC) Deployments. In Proceedings of the 14th ACM Symposium on Access Control Models and Technologies (SACMAT), Stresa, June 2009.

Bogdan Carbunar, Mahesh Tripunitara. Conditional Payments for Computing Markets. In Proceedings of the 7th International Conference on Cryptology and Network Security (CANS), Hong Kong, December 2008.

Peter Williams, Radu Sion, Bogdan Carbunar. Building Castles out of Mud: Practical Access Pattern Privacy and Correctness on Untrusted Storage. In Proceedings of the ACM Conference on Computer and Communication Security (CCS) [acceptance rate=15%], Alexandria, October 2008.

Bogdan Carbunar, Michael Pearce, Shivajit Mohapatra, Loren J. Rittle, Venu Vasudevan. Byzantine Resilient Synchronization for Content and Presence Updates in MANETS. In Proceedings of the 16th IEEE International Conference on Network Protocols (ICNP) [acceptance rate=16%], Orlando, October 2008.

Shivajit Mohapatra, Bogdan Carbunar, Michael Pearce, Rohit Chaudhri, Venu Vasudevan. Where-Fi: A Dynamic Energy-Efficient Multimedia Distribution Framework for MANETs. In Proceedings of the 15th SPIE/ACM Multimedia Computing and Networking (MMCN) [acceptance rate=26%], San Jose, January 2008.

Bogdan Carbunar, Yang Yu, Larry Shi, Michael Pearce, Venu Vasudevan. Query Privacy in Wireless Sensor Networks. In Proceedings of the 4th IEEE International Conference on Sensor and Ad Hoc Communications and Networks (SECON) [acceptance rate=20%], San Diego, June 2007.

Bogdan Carbunar, Brett Lindsley, Michael Pearce, Venu Vasudevan. Verifiable Credit Based Transfers in Wireless Ad Hoc Networks. In Proceedings of the 21st IEEE International Parallel and Distributed Processing Symposium (IPDPS) [acceptance rate=26%], Long Beach, March 2007.

Larry Shi, Bogdan Carbunar, Radu Sion. Conditional E-Cash. In Proceedings of the 11th Financial Cryptography and Data Security Conference (FC) [acceptance rate=18%], Tobago, February 2007.

Radu Sion, Bogdan Carbunar. On the Computational Practicality of Private Information Retrieval. In Proceedings of the 14th ISOC Network and Distributed System Security Symposium (NDSS) [acceptance rate=15%], San Diego, February 2007.

Bogdan Carbunar, Radu Sion. Uncheatable Reputation in Distributed Computation Markets. In Proceedings of the 10th Financial Cryptography and Data Security Conference (FC) [acceptance rate=29%], Anguilla, 2006.

Bogdan Carbunar, Murali Krishna Ramanathan, Mehmet Koyuturk, Christoph Hoffmann, Ananth Grama. Redundant Reader Elimination in RFID Systems. In Proceedings of the 2nd IEEE International Conference on Sensor and Ad Hoc Communications and Networks (SECON) [acceptance rate=27%], Santa Clara, September 2005.

Ioannis Ioannidis, Bogdan Carbunar, Cristina Nita-Rotaru. High Throughput Routing in Hybrid Cellular and Ad-Hoc Networks. In Proceedings of the 6th International Symposium on World of Wireless and Mobile Multimedia (IEEE WOWMOM), Taormina, June, 2005.

Bogdan Carbunar, Ananth Grama, Jan Vitek, Octavian Carbunar. Coverage Preserving Redundancy Elimination in Sensor Networks. In Proceedings of the 1st IEEE International Conference on Sensor and Ad Hoc Communications and Networks (SECON) [acceptance rate=18%], Santa Clara, October 2004.

Bogdan Carbunar, Ioannis Ioannidis, Ananth Grama, Jan Vitek. A Secure Crediting Protocol for Hybrid Cellular and Ad Hoc Networks. In Proceedings of the 1st International Conference on E-Business and Telecommunication Networks (ICETE), Setubal, August 2004.

Bogdan Carbunar, Ananth Grama, Jan Vitek. Distributed and Dynamic Voronoi Overlay Maintenance for Coverage Detection and Distributed Hash Tables in Ad Hoc Networks. In Proceedings of the 10th IEEE International Conference on Parallel and Distributed Systems (ICPADS), Long Beach, July 2004.

Bogdan Carbunar, Nitya Narasimhan, Venu Vasudevan. Boundary Tracking Solutions for Mobile Ad Hoc Networks. In Proceedings of Parallel and Distributed Computing and Systems (PDCS), Cambridge, November 4-6, 2002

Bogdan Carbunar, Marco Tulio Valente, Jan Vitek. Lime Revisited: Reverse Engineering An Agent Communication Model. In Proceedings of the 5th International Conference on Mobile Agents (MA2001), Atlanta, December 2-4, 2001

WORKSHOPS

Bogdan Carbunar, Radu Sion. Joining Privately on Outsourced Data. In Proceedings of the 7th VLDB Secure Data Management Workshop (SDM), Singapore, September 2010.

Yao Chen, Radu Sion, Bogdan Carbunar. XPay: Practical Anonymous Payments for TOR Routing and Other Networked Services. In Proceedings of the 8th ACM Workshop on Privacy in the Electronic Society (WPES), Chicago, November 2009.

Bogdan Carbunar, Ioannis Ioannidis, Cristina Nita-Rotaru. JANUS: Towards Secure and Malicious Resilient Routing in Hybrid Cellular and Ad-Hoc Networks. In Proceedings of the 3rd Workshop on Wireless Security (WiSe), held in conjunction with Mobicom [acceptance rate=25%], Philadelphia, October 2004.

Bogdan Carbunar, Marco Valente, Jan Vitek. CoreLime: A Coordination Model for Mobile Agents. In Proceedings of ConCoord: Workshop on Concurrency and Coordination, Lipari, July 6-8, 2001

POSTERS, DEMOS

Yao Chen, Radu Sion, Bogdan Carbunar. Anonymity and Privacy for Micropayments. In Proceedings of the 17th Usenix Security Symposium, San Jose, July 2008 (poster paper).

Radu Sion, Sumeet Bajaj, Bogdan Carbunar, Stefan Katzenbeisser. NS2: Networked Searchable Store with Correctness. In Proceedings of the 33rd International Conference on Very Large Data Bases (VLDB), Viena, September 2007 (demo paper).

Siddharth Bhatt, Bogdan Carbunar, Radu Sion, Venu Vasudevan. Personal Digital Rights Management for Mobile Cellular Devices. Systems paper in the 11th Financial Cryptography and Data Security Conference (FC) [acceptance rate=18%], Tobago, February 2007.

Radu Sion, Bogdan Carbunar. Mechanisms for Secure Reputation. Work in progress talk at the IEEE Symposium on Security and Privacy (SP), Oakland, May 2005.

Bogdan Carbunar, Ananth Grama, Jan Vitek. A Public Key Algorithm for Ad Hoc Networks (extended abstract/poster). In Proceedings of the 23rd IEEE International Performance Computing and Communications Conference, Phoenix, April 15-17, 2004.

Ioannis Ioannidis, Bogdan Carbunar. Scalable Routing in Hybrid Ad-Hoc and Cellular Networks (poster). In Proceedings of the 1st IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Fort Lauderdale, October 2004.

PATENT
DISCLOSURES

George Calcev, Bogdan Carbunar, Madjid Nakhjiri. Method and Apparatus for Dynamic Seamless Security in Communication Protocols. US7865717 B2. Issued February 2011.

Bogdan Carbunar, Yang Yu, Larry Shi, Michael Pearce. Method and Apparatus for Performing Anonymous Source Routing. US7532587 B2. Issued May 2009.

Bogdan Carbunar, Shivajit Mohapatra, Michael Pearce, Loren J. Rittle, Venugopal Vasudevan. Method and Apparatus for Synchronizing Nodes. USPTO Application Number 20100220747.

Yang Yu, Bogdan Carbunar, Zhu Li, Larry Shi. Method and Apparatus for Biometric Authentication Using Motion Sensor Enabled Mobile Devices. Filed by Motorola.

Brett Lindsley, Bogdan Carbunar, Mark Clayton, Venu Vasudevan. Method And System For Distributing Content In An Ad-Hoc P2P Environment Using Super-Peers. WO 2008048789 20080424.

SELECTED
PRESENTATIONS

Secure Synchronization of Periodic Updates in Ad Hoc Networks. School of Computing and Information Sciences, Florida International University (FIU), March 2011.

Secure Synchronization of Periodic Updates in Ad Hoc Networks. Computer Science Department, Worcester Polytechnic Institute (WPI), February 2011.

Secure Synchronization of Periodic Updates in Ad Hoc Networks. Computer Science Department, Purdue University, February 2011.

Regulatory Compliant Oblivious RAM. Palo Alto Research Center (PARC), August 2010.

Fair Payments for Outsourced Computations. IEEE SECON. Boston, June 2010.

Byzantine Resilient Synchronization for Content and Presence Updates in MANETs. IEEE ICNP, Orlando, October 2008.

Conditional Payments for Computing Markets. University of Chicago, May 2008.

Conditional E-Cash. University of Notre Dame, November 2007.

Verifiable Credit Based Transfers in Wireless Ad Hoc Networks. IEEE IPDPS, Long Beach, March 2007.

TEACHING
EXPERIENCE

Teaching Assistant: Graduate Level "Compilers", Purdue University, 2004.
Professor Antony Hosking
Graded assignments, projects, midterm and final exam.

Teaching Assistant: Graduate "Software Engineering", Purdue University, Spring and Fall 2000.
Professor Jan Vitek
Graded assignments, quizzes, midterm and final exam. Assisted students with projects and assignments.

Teaching Assistant: Undergraduate Level "Compilers", Purdue University, Fall 1999.
Professor Zhiyuan Li
Led lab sections and office hours assisting students with course material, projects and homework.
Graded assignments, midterm and final exam.

COMMUNITY
SERVICE

TPC Member: ISOC Network and Distributed System Security Symposium - NDSS 2012

TPC member: IEEE International Conference on Multimedia and Expo - IEEE ICME 2011

TPC member: ACM Workshop on Scalable Trusted Computing - ACM STC 2010

TPC member: ACM Cloud Computing Security Workshop - ACM CCSW 2010

TPC member: Financial Cryptography and Data Security - FC 2010

TPC member: Workshop on Scalable Trusted Computing - ACM STC 2009

TPC member: Cloud Computing Security Workshop - ACM CCSW 2009

TPC member: Workshop on Secure Network Protocols - IEEE NPSec 2009, 2008, 2007

TPC member: MODUS 2008

Poster chair: Financial Cryptography and Data Security - FC 2008

TPC member: Inscrypt 2007 (TPC member)

EXTERNAL REVIEW

IEEE Transactions on Computers (TC), IEEE Transactions on Parallel and Distributed Systems (TPDS), IEEE Transactions on Mobile Computing (TMC), IEEE Transactions on Wireless Computing (TWC), ACM Transactions on Sensor Networks, Parallel Processing Letters (PPL), International Journal of Web Engineering and Technology (IJWET), ACNS 2010, IEEE ICNP 2008, ACM CCS 2008, IEEE ICC, ACM SIGMOD 2008, IEEE ICDCS 2007, IEEE Globecom 2007, MSWiM 2007, IEEE WCNC 2007, IEEE INFOCOM 2004, IEEE ICDCS 2004, IEEE CEC 2004, ECOOP 2002