Christopher A. Wood

Permanent Address
2000 Post St., Apt. 123
San Francisco, CA 94115

Phone: (315) 806-5939
Email: woodc1@uci.edu
www.christopher-wood.com

RESEARCH INTERESTS

Content-centric networking architectures and protocols, computer and network security and privacy, cryptographic algorithms and engineering, software engineering, and heterogeneous computing.

EDUCATION

Doctor of Philosophy, Computer Science
University of California Irvine, Irvine, CA — 2013 - 2018 (expected)
Advisors: Dr. Gene Tsudik
GPA: 4.0/4.0

Master of Science, Computer Science
Rochester Institute of Technology, Rochester, NY — 2012 - 2013
Thesis: Large Substitution Boxes with Efficient Combinational Implementations
Advisor: Dr. Stanisław Radziszowski
GPA: 4.0/4.0

Bachelor of Science, Computer Science and Software Engineering
Rochester Institute of Technology, Rochester, NY — 2008 - 2012
Concentrations: Computational Mathematics and Computer Engineering
Minor: Mathematics
GPA: 3.98/4.0 (Professional Field of Study GPA: 4.0/4.0)

PUBLICATIONS

Journal Articles

J-1. P. Bajorski, A. Kaminsky, M. Kurdziel, M. Lukowiak, S. Radziszowski, and C. Wood, "Stochastic Analysis and Modeling of a Tree-Based Group Key Distribution Method in Tactical Wireless Networks," to appear in *Journal of Telecommunications System & Management, Engineering Journals, OMICS Publishing Group*.

J-2. C. A. Wood and J. Jacob, "Characterization of Small Trees Based on their L(2,1)-Span," to appear in the *AKCE International Journal of Graphs and Combinatorics*.

J-3. M. Lukowiak, S. Radziszowski, J. Vallino, C. Wood, "Cybersecurity Education: Bridging the Gap between Hardware and Software Domains," *ACM Transactions on Computing Education*, 14(1) (2014).

Conference Proceedings

C-1. G. Tusik, E. Uzun, and C. A. Wood, "AC3N: An API and Service for Anonymous Communication in Content-Centric Networking," in *Proceedings of CCNC 2016*, Las Vegas, NV, USA. January 2016.

C-2. C. A. Wood, S. P. Radziszowski, and M. Lukowiak, "Constructing Large S-boxes with Area Minimized Implementations," in *Proceedings of MILCOM'2015*, Tampa, FL, USA. October 2015.

C-3. M. Mosko and C. A. Wood, "Secure Fragmentation for Content-Centric Networking," *IEEE MASS 2015 Workshop on Content-Centric Networking (CCN 2015)*, Dallas, TX, USA. October 2015.

C-4. C. Ghali, M. A. Schlosberg, G. Tsudik, and C. A. Wood, "Interest-Based Access Control for Information Centric Networks," in *Proceedings of ICN 2015, the 2nd ACM Conference on Information Centric Networking*, San Francisco, CA, USA. September 2015.

C-5. C. Ghali, A. Narayanan, D. Oran, G. Tsudik, and C. A. Wood, "Secure Fragmentation for Content-Centric Networks," *NCA 2015, the 14th IEEE International Symposium on Network Computing and Applications*, Cambridge, MA, USA. September 2015.

C-6. J. Kurihara, C. A. Wood, and E. Uzun, "An Encryption-Based Access Control Framework for Content-Centric Networking," *IFIP Networking 2015*, Toulouse, France. May 2015.

C-7. S. Skalicky, S. Lopez, M. Lukowiak, and C. A. Wood, "Mission Control: A Performance Metric and Analysis of Control Logic for Pipelined Architectures on FPGAs," to appear in *Proceedings of the 2014 International Conference on Reconfigurable Computing and FPGAs - ReConFig 2014*, Cancun, Mexico. December 2014.

C-8. C. A. Wood and E. Uzun, "Flexible End-to-End Content Security in CCN," *IEEE Consumer Communications and Networking Conference (CCNC 2014) Special Session: Information Centric Networking*, Las Vegas, Nevada. January 2014.

C-9. S. Skalicky, C. A. Wood, M. Lukowiak, and M. Ryan, "High Level Synthesis: Where Are We? A Case Study on Matrix Multiplication," in *Proceedings of the 2013 International Conference on Reconfigurable Computing and FPGAs - ReConFig 2013*, Cancun, Mexico. December 2013.

C-10. M. Lukowiak, A. Meneely, S. Radziszowski, J. Vallino, and C. Wood, "Developing an Applied, Security-Oriented Computing Curriculum," in *Proceedings of the ASEE 2012*, San Antonio, Texas. June 2012.

C-11. C. A. Wood, "Chaos-Based Symmetric Key Cryptosystems," in *Proceedings of the 2011 International Conference on Security & Management*, Las Vegas, Nevada. July 2011.

C-12. C. A. Wood and R. K. Raj, "Keyloggers in Cybersecurity Education," in *Proceedings of the 2010 International Conference on Security & Management*, Las Vegas, Nevada. July 2010.

Theses

T-1. C. A. Wood, "Large Substitution Boxes with Efficient Combinational Implementations," M.S. Thesis, Computer Science, Rochester Institute of Technology, Rochester, NY. August 2013.

Surveys

S-1. C. A. Wood, "Small Folkman Numbers." *Draft available online:* `http://christopher-wood.com/papers/FolkmanSurvey.pdf`.

Technical Reports

TR-1. M. Mosko, I. Solis, E. Uzun, and C. A. Wood, "CCNx 1.0 Protocol Architecture," Technical report, August, 2015. Available online at `http://www.ccnx.org/pubs/CCNxProtocolArchitecture.pdf`.

TALKS AND PRESENTATIONS

P-1. "Efficient Security Bindings for Information Centric Networks," *CCNxCon 2015, Palo Alto Research Center, Palo Alto, CA*. May 20, 2015.

P-2. "Handling Trust Enforcement," presentation, *CCNxCon 2015, Palo Alto Research Center, Palo Alto, CA*. May 20, 2015.

P-3. "Digital Signatures and Implicit Certificates," guest lecture for Dr. Stanislaw Radziszowski's (CS@RIT), Crypto II course, May 5, 2015.

P-4. "On the $L(2,1)$ Labeling of Trees," with Jobby Jacob (presenter), *Joint Mathematics Meetings*, Baltimore, MD. January 15-18, 2014.

P-5. "Secure Content Dissemination in Content Centric Networking," *CCNxCon 2013, Palo Alto Research Center, Palo Alto, CA*. September 5, 2013.

P-6. "Cryptographic S-boxes," guest lecture for Dr. Stanislaw Radziszowski's (CS@RIT) Crypto II course, April 8, 2013.

P-7. "Characterization Results for the L(2,1)-Labeling Problem on Trees," *AMS Sectional Meeting, RIT, Rochester, NY.* September 22, 2012.

P-8. "Chaos-Based Symmetric Key Cryptosystems," *RIT Graduate Research Symposium, RIT, Rochester, NY.* July 22, 2011.

P-9. "Layered Driver Rootkit Detection on Microsoft Windows PCs," *RIT Undergraduate Research Symposium, RIT, Rochester, NY.* August 24, 2009.

PATENTS

F-1. I. Solis, G. Scott, C. Wood, "Content Negotiation in CCN," filed.

F-2. G. Scott, C. Wood, "Transport Stack Name Scheme and Identity Management," filed.

F-3. G. Scott, C. Wood, "Flexible Command and Control In CCN," filed.

F-4. J. Kurihara, E. Uzun, C. Wood, "Access Control Framework for Content Centric Networking," filed.

F-5. M. Mosko, E. Uzun, C. Wood, "Trust Enforcement Framework for Content Centric Networking," filed.

F-6. M. Mosko, I. Solis, G. Scott, C. Wood, "Order Encoded Manifests," filed.

F-7. P. Bajorski, A. Kaminsky, M. Kurdziel, M. Lukowiak, S. P. Radziszowski, and C. Wood, "Electronic Key Management Using PKI to Support Group Key Establishment in the Tactical Environment, " U.S. Patent Number 8,873,759. October 28, 2014.

PROFESSIONAL EXPERIENCE

Palo Alto Research Center — September 2014 - present
Computer Science Laboratory, Palo Alto, CA — Network Software Development Engineer

- Develop the CCNx 1.0 software stack and APIs.
- Implement internal code measurement tools for quantifiable software quality improvements.
- Write IETF RFC drafts for various elements of the CCN protocol.
- Contribute to CCN-related patent portfolio.

Palo Alto Research Center — June 2014 - September 2014
Computer Science Laboratory, Palo Alto, CA — Security and Privacy Research Intern

- Designed flexible manifest-based access control framework for CCNx 1.0.
- Designed and implemented network-layer trust enforcement mechanics in CCNx 1.0.
- Implemented various encryption-based access control primitives, including Broadcast Encryption and Proxy Re-Encryption for CCNx 1.0.

Cigital, Inc. — March 2014 - July 2014
Dulles, MD — Security Consultant Contractor

- Focused on security-oriented C/C++ source code review and application architectural analyses.

Palo Alto Research Center — July 2013 - September 2013
Computer Science Laboratory, Palo Alto, CA — Security and Privacy Research Intern

- Researched security and privacy aspects related to content-centric network (CCN).
- Implemented the Green-Ateniese (pairing-based) and Chow-Weng-Yang-Deng (Schnorr- and ElGamal-based) Proxy Re-Encryption schemes in Java for use in a CCNx application.
- Studied and tested various techniques for securing content that is distributed throughout a CCN mesh for confidentiality purposes.
- Experimented with techniques for improving name privacy in CCN.

Intel Corporation — June 2012 - August 2012
Virtual & Parallel Computing Group, Folsom, CA — Graphics Software Engineer Intern

– Developed production features for tool that processes hardware specifications to generate web content and source code for VHDL and C/C++ testbeds.
– Interacted with internal customers within the VPG to utilize debug tools and environments for architecture specification and post-silicon testing.

L-3 Communications March 2011 - August 2011
Victor, NY Software Engineer Intern
– Designed and implemented a library and supporting drivers for the μ-blox NEO5/6 GPS receiver driven by an Analog Devices Blackfin processor.
– Extended an existing FAT file system driver to add support for SD devices.
– Improved functionality of a CPLD controller for an embedded power supply.

Rochester Software Associates November 2010 - March 2011
Rochester, NY Software Engineer Intern
– Led the design, development, and documentation efforts for a new printer job management application that would service any number of jobs from clients across the network.
– Tested and debugged an existing .NET implementation of an LPD client.

C Speed, LLC May 2010 - August 2010
Liverpool, NY Software Engineer Intern
– Designed and implemented an internal manufacturing part supply management system.
– Implemented embedded firmware features and test routines in C, C++, and assembly for Coldfire V2 processors.

ACADEMIC EXPERIENCE

Advanced Cryptography May 5, 2015
Guest Lecturer for Dr. Stanisław Radziszowski (CS) (RIT)
– Lectured about digital signature algorithms, ElGamal and ECDSA batch verification techniques, standard public key infrastructures, and the OMC and ECQV implicit certificate schemes.

Cryptography II April 8, 2013
Guest Lecturer for Dr. Stanisław Radziszowski (CS) (RIT)
– Lectured about recent research on the security and (hardware) implementation efficiency of cryptographic S-boxes.

Hardware and Software Design with Cryptographic Applications February 2011 - May 2013
Teaching Assistant and Lecturer for Dr. Marcin Lukowiak (CE) (RIT)
– Developed and delivered lecture material on cryptography, embedded software optimization techniques, the Impulse C high-level synthesis tool, and AES cache timing attacks.
– Assisted students with weekly assignments and graded lab and project deliverables.

Computer Science I, II, and IV January 2009 - May 2013
Student Lab Assistant and Grader (RIT)
– Proctored problem solving sessions and ran lab meetings with lectures of weekly material.
– Graded weekly lab assignments and midterm examinations.

Personal Software Engineering December 2011 - March 2012
Teaching Assistant for Professor Tom Reichlmayr (SE) (RIT)
– Assisted students with in-class programming assignments and course projects.
– Graded projects written in C/C++ and Ruby (with Ruby on Rails).

Engineering of Software Subsystems September 2011 - December 2011
Teaching Assistant for Dr. James Vallino (SE) (RIT)

– Assisted students with in-class exercises and unit questions based on a subset of the design patterns taught during the course.
– Spent time with each student team to discuss course projects, including design decisions, application of design patterns, and alternatives considered.

TECHNICAL SKILLS

– Programming Languages: C/C++, C#, Java, Python, Scala, Ruby, Assembly (MIPS), JavaScript, Objective-C, Standard ML, Scheme
– Modeling Languages and Tools: VHDL, Verilog, UML, SPIN (with PROMELA), Alloy
– Specialized Software: MATLAB, Mathematica, WEKA, Magma, Sage, LLVM
– Markup Languages: LaTeX, HTML(5), CSS3
– Web Frameworks: NodeJS, Spring MVC, Ruby on Rails

MEMBERSHIPS

IEEE, Student Member
ACM, Student Member
SIAM, Student Member
IACR, Student Member
Internet Society, Member
Tau Beta Pi, Member

HONORS AND ACTIVITIES

– NSF GRFP fellowship recipient, 2014
– RIT Honors Program, 2009 – 2013
– RIT Tau Beta Pi Engineering Honors Society, 2011 – 2013
– RIT Outstanding Undergraduate Student award, selected, Winter 2012
– RIT Computer Science MS Student Delegate, selected, Winter 2012
– Recipient of Golisano College Honors research assistantship stipend, Winter 2009/2010
– Recipient of Golisano College Honors research assistantship stipend, Spring 2011
– Recipient of RIT undergraduate research award stipend, Summer 2009
– RIT Golisano College Dean's List, 2008 – 2013
– Student mentor for the FIRST LEGO League team hosted by RIT, Fall 2009 – Winter 2010
– Rochester Foodlink volunteer, Winter 2012/2013 – March 2013
– Society of Software Engineers, member, Fall 2008 – Winter 2009/2010
– RIT Electronic Gaming Society, member, Fall 2008 – Spring 2010
– RIT Intramural Flag Football Team, member, Fall 2010

INTERESTS

Guitar, running, cycling, swimming, languages, and the natural sciences.