# Christopher A. Wood

**Permanent Address**
65 W 5th Avenue, Apt. 218
San Mateo, CA 94402

Phone: (315) 806-5939
Email: woodc1@uci.edu
Website: `www.caw.fyi`

## RESEARCH INTERESTS

Computer and network security and privacy, cryptographic algorithms and engineering, network architectures, software engineering, and heterogeneous computing.

## EDUCATION

*Doctor of Philosophy*, Computer Science
University of California Irvine, Irvine, CA — 2013 - 2017 (expected)
Advisor: 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
mConcentrations: Computational Mathematics and Computer Engineering
Minor: Mathematics
GPA: 3.98/4.0 (Professional Field of Study GPA: 4.0/4.0)

## PUBLICATIONS

### Conference Proceedings

C-1. C. Ghali, G. Tsudik, C. A. Wood, "(The Futility of) Data Privacy in Content-Centric Networking," to appear in the *2016 Workshop on Privacy in the Electronic Society* (WPES 2016), October 24, 2016, Vienna, Austria.

C-2. C. Ghali, G. Tsudik, C. A. Wood, "Network Names in Content-Centric Networking," to appear in the *3rd ACM Conference on Information-Centric Networking (ICN 2016)*, Sept. 26 - 28, 2016, Kyoto, Japan.

C-3. C. Tschudin, E. Uzun, C. A. Wood, "Trust in Information-Centric Networking: From Theory to Practice," in *Proceedings of the 25th International Conference on Computer Communication and Networks (ICCCN 2016)*, August 1 - 4, 2016, Waikoloa, Hawaii, USA.

C-4. C. Ghali, G. Tsudik, C. A. Wood, "BEAD: Best Effort Autonomous Deletion in Content-Centric Networking," *FIP Networking 2016*, May 17 - 19, 2016, Vienna, Austria.

C-5. C. Ghali, G. Tsudik, C. A. Wood, E. Yeh, "Practical Accounting in Content-Centric Networking," *NOMS 2016, IEEE/IFIP Network Operations and Management Symposium*, April 25 - 29, 2016, Istanbul, Turkey.

C-6. G. Tsudik, 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-7. 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-8. 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-9. 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-10. 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. (Best paper award winner)

C-11. 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-12. 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-13. 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-14. 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-15. 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-16. C. A. Wood, "Chaos-Based Symmetric Key Cryptosystems," in *Proceedings of the 2011 International Conference on Security & Management*, Las Vegas, Nevada. July 2011.

C-17. 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.

**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," *AKCE International Journal of Graphs and Combinatorics*, Volume 12, Issue 1, July 2015, Pages 2631.

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).

**Posters**

P-1. C. A. Wood and G. Scott, "A Network-Agnostic Data Framework and API for CCN," ICN 2015, the 2nd ACM Conference on Information Centric Networking, September 30 - October 2, 2015, San Francisco, CA, USA.

P-2. M. Mosko, G. Scott, I. Solis, and C. A. Wood, "Secure Prefix Registration in CCN," ICN 2015, the 2nd ACM Conference on Information Centric Networking, September 30 - October 2, 2015, San Francisco, CA, USA.

**Theses**

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

**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

T-1. "Access Control in Information-Centric Networks," presentation, Invited Talk at SRI, Menlo Park, CA, USA, August 17, 2016.

T-2. "File-Like ICN Collection (FLIC)," presentation, ICNRG Meeting, Berlin, Germany, July 21, 2016.

T-3. "CCNx Testrig," presentation, ICNRG Interim Meeting, Berlin, Germany, July 17, 2016.

T-4. "Secure Transport Offload with Encrypted PEPs," presentation, ICNRG Interim Meeting, Berlin, Germany, July 17, 2016.

T-5. "Group Key Encryption," presentation, ICNRG Interim Meeting, Berlin, Germany, July 17, 2016.

T-6. "CDN Architecture Pain Points and ICN Cures?," presentation, ICNRG Interim Meeting, Berlin, Germany, July 17, 2016.

T-7. "Let's Check Let's Encrypt: A Tool for Code-Driven Threat Modeling," presentation, BSidesROC, Rochester, NY, USA. April 23, 2016.

T-8. "Session-Based Content Distribution with CCNx-KE," presentation, ICNRG Interim Meeting, Buenos Aires, Argentina. April 3, 2016.

T-9. "CCNx-KE vs (D)TLS," presentation, ICNRG Interim Meeting, Buenos Aires, Argentina. April 3, 2016.

T-10. ""Private Communication in ICN," presentation, ICNRG Interim Meeting, Buenos Aires, Argentina. April 3, 2016.

T-11. "TLV Encryption and Packet Encapsulation," presentation, ICNRG Interim Meeting, Paris, France. January 15, 2016.

T-12. "CCNx Key Exchange - Updates," presentation, ICNRG Interim Meeting, Paris, France. January 15, 2016.

T-13. "FLIC Manifests," presentation, ICNRG Interim Meeting, Paris, France. January 14, 2016.

T-14. "CCNx Key Exchange," presentation, IETF 94 ICNRG Meeting, Yokohama, Japan. November 4, 2015.

T-15. "Static Manifest Requirements," presentation, IETF 94 ICNRG Meeting, Yokohama, Japan. November 4, 2015.

T-16. "CCNx over UDP," presentation, IETF ICNRG Interim Meeting, San Francisco, CA. October 3, 2015.

T-17. "Manifests," presentation, IETF ICNRG Interim Meeting, San Francisco, CA. October 3, 2015.

T-18. "Efficient Security Bindings for Information Centric Networks," *CCNxCon 2015, Palo Alto Research Center, Palo Alto, CA*. May 20, 2015.

T-19. "Handling Trust Enforcement," presentation, *CCNxCon 2015, Palo Alto Research Center, Palo Alto, CA*. May 20, 2015.

T-20. "Digital Signatures and Implicit Certificates," guest lecture for Dr. Stanislaw Radziszowski's (CS@RIT), Crypto II course, May 5, 2015.

T-21. "On the $L(2,1)$ Labeling of Trees," with Jobby Jacob (presenter), *Joint Mathematics Meetings*, Baltimore, MD. January 15-18, 2014.

T-22. "Secure Content Dissemination in Content Centric Networking," *CCNxCon 2013, Palo Alto Research Center, Palo Alto, CA*. September 5, 2013.

T-23. "Cryptographic S-boxes," guest lecture for Dr. Stanislaw Radziszowski's (CS@RIT) Crypto II course, April 8, 2013.

T-24. "Characterization Results for the L(2,1)-Labeling Problem on Trees," *AMS Sectional Meeting, RIT, Rochester, NY.* September 22, 2012.

T-25. "Chaos-Based Symmetric Key Cryptosystems," *RIT Graduate Research Symposium, RIT, Rochester, NY.* July 22, 2011.

T-26. "Layered Driver Rootkit Detection on Microsoft Windows PCs," *RIT Undergraduate Research Symposium, RIT, Rochester, NY.* August 24, 2009.

## PROFESSIONAL EXPERIENCE

*Apple, Inc.* October 2016 - present
CoreOS, Cupertino, CA Secure Transport Engineer
- Work on the CoreOS TLS and IPsec implementations.

*Palo Alto Research Center* September 2014 - October 2016
Computer Science Laboratory, Palo Alto, CA Software Engineer and Researcher
- Developed the CCNx 1.0 network stack, security libraries, APIs, and applications.
- Lead CCNx technical meetings and drove IRTF RFC drafts for the ICNRG.
- Contributed to the PARC CCN patent portfolio.
- Implemented internal code measurement tools for quantifiable software quality improvements.

*Palo Alto Research Center* June 2014 - September 2014
Computer Science Laboratory, Palo Alto, CA Security and Privacy Research Intern
- Designed manifests and a manifest-based access control framework for CCNx.
- Implemented encryption-based access control modules based on Broadcast Encryption and Proxy Re-Encryption for CCNx.
- Designed and implemented trust enforcement mechanics in the transport stack for CCNx.

*Cigital, Inc.* March 2014 - July 2014
Dulles, MD Security Consultant Contractor
- Contributed to security-oriented C/C++ source code review and 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.
- 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 $\mu$-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.

## 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.