

## Christopher A. Wood

### Permanent Address

1140 Lovell Ave  
Campbell, CA 95008

Phone: (315) 806-5939  
Email: [caw@heapingbits.net](mailto:caw@heapingbits.net)  
Website: [www.caw.fyi](http://www.caw.fyi)

### RESEARCH INTERESTS

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

### EDUCATION

*Doctor of Philosophy*, Computer Science  
University of California Irvine, Irvine, CA 2013 - 2017  
Thesis: Security and Privacy Challenges in Content-Centric Networks  
Advisor: Dr. Gene Tsudik

*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

*Bachelor of Science*, Computer Science and Software Engineering  
Rochester Institute of Technology, Rochester, NY 2008 - 2012  
Concentrations: Computational Mathematics and Computer Engineering  
Minor: Mathematics

### PROFESSIONAL EXPERIENCE

*Apple, Inc.* October 2018 - present  
Cupertino, CA Senior Software Engineer

- Lead TLS efforts across Apple.
- Design and develop security protocols and technologies for protecting user data.
- Assist cryptographic engineering team with the development of cryptographic algorithms and quality-related projects.

*Apple, Inc.* October 2016 - October 2018  
Cupertino, CA Software Engineer

- Took ownership the Apple client-side TLS stack(s). Primarily focused on replacing coreTLS with BoringSSL on Apple platforms.
- Shipped TLS 1.3 by default and took steps towards removing support for TLS 1.0 and 1.1 on Apple products.
- Helped ship Network.framework with built-in TLS support.
- Developed internal cryptographic APIs and implemented algorithms for CloudKit and related technologies.
- Led security-related standardization efforts in the IETF and IRTF, focusing on TLS extensions and foundation cryptographic protocols.
- Developed proof-of-concept code quality and test coverage regression system for the Security Engineering and Architecture organization.

*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.
- Led 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.

## ACADEMIC EXPERIENCE

*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.

- Assisted students with in-class programming assignments and course projects.
- Graded projects written in C/C++ and Ruby (with Ruby on Rails).

- 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.

## PUBLICATIONS AND STANDARDIZATION WORK

### Conference Proceedings

- C-1. I. Oliviera-Nunes, G. Tsudik, and C. A. Wood, "Namespace Tunnels in Content-Centric Networks," *42nd Annual IEEE Conference on Local Computer Networks (LCN 2017)*, October 9 - 12, 2017, Singapore.
- C-2. C. Ghali, G. Tsudik, and C. A. Wood, "Mitigating On-Path Adversaries in Content-Centric Networks," *42nd Annual IEEE Conference on Local Computer Networks (LCN 2017)*, October 9 - 12, 2017, Singapore.
- C-3. C. Ghali, G. Tsudik, and C. A. Wood, "When Encryption is Not Enough: Privacy Attacks in Content-Centric Networking," to appear in the *4th ACM Conference on Information-Centric Networking (ICN 2017)*, September 26 - 28, 2017, Berlin, Germany.
- C-4. C. Ghali, G. Tsudik, E. Uzun, and C. A. Wood, "Closing the Floodgate with Stateless Content-Centric Networking," to appear in the *26th International Conference on Computer Communication and Networks (ICCCN 2017)*, July 31 - August 3, 2017, Vancouver, Canada. **(Best paper award)**
- C-5. C. A. Wood, "Protecting the Long Tail: Transparent Packet Security in Content-Centric Networks," *IFIP Networking 2017*, June 12-16, 2017, Stockholm, Sweden.
- C-6. M. Mosko, E. Uzun, and C. A. Wood, "Mobile Sessions in Content-Centric Networks," *IFIP Networking 2017*, June 12-16, 2017, Stockholm, Sweden.
- C-7. M. Mosko, C. A. Wood, "Secure Off-Path Replication in Content-Centric Networks," *IEEE ICC 2017 Next Generation Networking and Internet Symposium (NGNI 2017)*, May 21-25, 2017, Paris, France.
- C-8. C. Ghali, G. Tsudik, C. A. Wood, "(The Futility of) Data Privacy in Content-Centric Networking," *2016 Workshop on Privacy in the Electronic Society (WPES 2016)*, October 24, 2016, Vienna, Austria.
- C-9. C. Ghali, G. Tsudik, C. A. Wood, "Network Names in Content-Centric Networking," *3rd ACM Conference on Information-Centric Networking (ICN 2016)*, Sept. 26 - 28, 2016, Kyoto, Japan.
- C-10. C. Tschudin, E. Uzun, C. A. Wood, "Trust in Information-Centric Networking: From Theory to Practice," *Proceedings of the 25th International Conference on Computer Communication and Networks (ICCCN 2016)*, August 1 - 4, 2016, Waikoloa, Hawaii, USA.
- C-11. 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-12. 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-13. G. Tsudik, E. Uzun, and C. A. Wood, "AC3N: An API and Service for Anonymous Communication in Content-Centric Networking," *Proceedings of CCNC 2016*, Las Vegas, NV, USA. January 2016.
- C-14. C. A. Wood, S. P. Radziszowski, and M. Lukowiak, "Constructing Large S-boxes with Area Minimized Implementations," *Proceedings of MILCOM'2015*, Tampa, FL, USA. October 2015.

- C-15. 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-16. C. Ghali, M. A. Schlosberg, G. Tsudik, and C. A. Wood, "Interest-Based Access Control for Information Centric Networks," *Proceedings of ICN 2015, the 2nd ACM Conference on Information Centric Networking*, San Francisco, CA, USA. September 2015.
- C-17. 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)**
- C-18. 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-19. 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," in *Proceedings of the 2014 International Conference on Reconfigurable Computing and FPGAs - ReConFig 2014*, Cancun, Mexico. December 2014.
- C-20. 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-21. S. Skalicky, C. A. Wood, M. Lukowiak, and M. Ryan, "High Level Synthesis: Where Are We? A Case Study on Matrix Multiplication," *Proceedings of the 2013 International Conference on Reconfigurable Computing and FPGAs - ReConFig 2013*, Cancun, Mexico. December 2013.
- C-22. M. Lukowiak, A. Meneely, S. Radziszowski, J. Vallino, and C. Wood, "Developing an Applied, Security-Oriented Computing Curriculum," *Proceedings of the ASEE 2012*, San Antonio, Texas. June 2012.
- C-23. C. A. Wood, "Chaos-Based Symmetric Key Cryptosystems," *Proceedings of the 2011 International Conference on Security & Management*, Las Vegas, Nevada. July 2011.
- C-24. C. A. Wood and R. K. Raj, "Keyloggers in Cybersecurity Education," *Proceedings of the 2010 International Conference on Security & Management*, Las Vegas, Nevada. July 2010.

## Journal Articles

- J-1. G. Acs, M. Conti, P. Gasti, C. Ghali, G. Tsudik, and C. A. Wood, "Privacy-Aware Caching in Information-Centric Networking," *IEEE Transactions on Dependable and Secure Computing*.
- J-2. E. Ngai, B. Ohlman, G. Tsudik, E. Uzun, M. Wahlsch, C. A. Wood, "Can We Make a Cake and Eat It Too? A Discussion of ICN Security and Privacy," *ACM SIGCOMM Computer Communication Review*, Volume 47 Issue 1, January 2017, Pages 49-54.
- J-3. 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," *Journal of Telecommunications System & Management, Engineering Journals, OMICS Publishing Group*.
- J-4. 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 26-31.
- J-5. 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).

## Internet Drafts

- D-1. N. Sullivan, and C. A. Wood, "Hashing to Elliptic Curves," Internet Draft, March, 2018.
- D-2. N. Sullivan, and C. A. Wood, "Verifiable Oblivious Pseudorandom Functions (VOPRFs)," Internet Draft, March, 2018.
- D-3. C. Cremers, L. Garratt, S. Smyshlyaev, N. Sullivan, and C. A. Wood, "Randomness Improvements for Security Protocols," Internet Draft, March, 2018.

- D-4. B. Trammell, M. Welzl, T. Enghardt, G. Fairhurst, M. Kuehlewind, C. Perkins, P. Tiesel, C. Wood, "An Abstract Application Layer Interface to Transport Services," Internet Draft, March, 2018.
- D-5. T. Pauly, B. Trammell, A. Brunstrom, G. Fairhurst, C. Perkins, P. Tiesel, C. Wood, "An Architecture for Transport Services," Internet Draft, March, 2018.
- D-6. M. Kuehlewind, T. Pauly, C. A. Wood, "Separating Crypto Negotiation and Communication," Internet Draft, March, 2018.
- D-7. T. Pauly, C. Perkins, K. Rose, C. A. Wood, "A Survey of Transport Security Protocols," Internet Draft, March, 2018.
- D-8. B. Trammell, C. Perkins, M. Kuehlewind, T. Pauly, C. A. Wood, "Post Sockets, An Abstract Programming Interface for the Transport Layer," Internet Draft, October, 2017.
- D-9. M. Mosko, I. Solis, and C. A. Wood, "CCNx Semantics," Internet Draft, October, 2017.
- D-10. M. Mosko, I. Solis, and C. A. Wood, "CCNx Messages in TLV Format," Internet Draft, October, 2017.
- D-11. B. Wissingh, C. A. Wood, A. Afanasyev, L. Zhang, D. Oran, C. Tschudin, "Information-Centric Networking (ICN): CCN and NDN Terminology," Internet Draft, September, 2017.
- D-12. M. Mosko and C. A. Wood, "The CCNx URI Scheme," Internet Draft, October, 2016.
- D-13. M. Mosko, E. Uzun, and C. A. Wood, "CCNx Key Exchange Protocol Version 1.0," Internet Draft, July, 2017.
- D-14. M. Mosko and C. A. Wood, "Encrypted Sessions In CCNx (ESIC)," Internet Draft, September, 2017.
- D-15. C. Tschudin and C. A. Wood, "File-Like ICN Collection (FLIC)," Internet Draft, June, 2017.
- D-16. C. A. Wood, "Content-Locked Encryption and Authentication of Nameless Objects," Internet Draft, September, 2017.

## 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.

## Technical Reports

- TR-1. M. Mosko, I. Solis, and C. A. Wood, "Content-Centric Networking - Architectural Overview and Protocol Description," June 22, 2017. Available online at <https://arxiv.org/abs/1706.07165>.
- TR-2. E. Ngai, B. Ohlman, G. Tsudik, E. Uzun, and C. A. Wood, "Information-centric Networking and Security (Dagstuhl Seminar 16251)," Dagstuhl Reports. Vol. 6. No. 6. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik (2016). Available online at [http://drops.dagstuhl.de/opus/volltexte/2016/6727/pdf/dagrep\\_v006\\_i006\\_p049\\_s16251.pdf](http://drops.dagstuhl.de/opus/volltexte/2016/6727/pdf/dagrep_v006_i006_p049_s16251.pdf).
- TR-3. C. Ghali, G. Tsudik, E. Uzun, C. A. Wood, "Living in a PIT-less World: A Case Against Stateful Forwarding in Content-Centric Networking," December 24, 2015. Available online at <https://arxiv.org/abs/1512.07755>.
- TR-4. C. Ghali, G. Tsudik, C. A. Wood, E. Yeh, "Practical Accounting in Content-Centric Networking (extended version)," October 7, 2015. Available online at <https://arxiv.org/abs/1510.01852>.
- TR-5. C. Ghali, M. A. Schlosberg, G. Tsudik, C. A. Wood, "Interest-Based Access Control for Content Centric Networks (extended version)," May 23, 2015. Available online at <https://arxiv.org/abs/1505.06258>.
- TR-6. G. Scott and C. A. Wood, "Network-Agnostic Systems in a Networked World," August 1, 2014. Available online at [https://www.christopher-wood.com/docs/reports/icn\\_layers15.pdf](https://www.christopher-wood.com/docs/reports/icn_layers15.pdf).

- TR-7. C. Ghali, A. Narayanan, D. Oran, G. Tsudik, C. A. Wood, "Secure Fragmentation for Content-Centric Networks (extended version)," May 12, 2014. Available online at <https://arxiv.org/abs/1405.2861>.
- TR-8. G. Tsudik, E. Uzun, and C. A. Wood, "AC3N - An API and Service for Anonymous Communication in Content-Centric Networking," May 1, 2014. Available online at <https://www.christopher-wood.com/docs/reports/ac3n14.pdf>
- TR-9. G. Scott and C. A. Wood, "Application-Layer Gateway for IP and Content Centric Network Interoperability," January 1, 2014. Available online at <https://www.christopher-wood.com/docs/reports/ccnsink14.pdf>.

## **MEMBERSHIPS**

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

## **HONORS AND ACTIVITIES**

- NSF GRFP fellowship recipient, 2014
- RIT Honors Program, 2009 – 2013
- RIT Golisano College Dean's List, 2008 – 2013
- RIT Tau Beta Pi Engineering Honors Society, 2011 – 2013
- RIT Computer Science Graduate Student Delegate, selected, Winter 2012
- RIT Outstanding Undergraduate Student Award, 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 stipend, Summer 2009