Christopher A. Wood

71-4 Lilac Drive
Rochester, NY 14620

October 4, 2012

caw4567@rit.edu
www.christopher-wood.com

Academic Information

- **Rochester Institute of Technology** Rochester, NY
  M.S. Computer Science *2012 – 2013 (expected)*
  - Advisor: Stanisław Radziszowski
  - Thesis: Optimal Representations of Cryptographic Substitution Boxes for Efficient Combinational Implementations (in progress)
  - GPA: 4.0/4.0
  - Thesis-related courses: Cryptography, Intelligent Security Systems, Data Communications and Networks, Algorithms, Optimization Methods

- **Rochester Institute of Technology** Rochester, NY
  B.S. Computer Science and Software Engineering *2008 – 2012*
  - Concentrations: Computational Mathematics and Computer Engineering
  - Minors: Mathematics and Writing Studies
  - GPA: 3.97/4.0 (Primary Field of Study GPA: 4.0/4.0)
  - Main electives: Graph Theory, Number Theory, Operating Systems, Programming Language Concepts, Computer Organization, Modern Physics, Real-Time and Embedded Systems

Publications (available at www.christopher-wood.com)

Journal Articles

J-1. C. Wood and J. Jacob, "Forbidden Subtree Construction Techniques for Trees Under the $L(2,1)$-Labeling Problem on Trees," *in preparation*.

J-2. C. Wood and J. Jacob, "Characterization Results for the $L(2,1)$-Labeling Problem on Trees," *in preparation*.

J-3. P. Bajorski, A. Kaminsky, M. Kurdziel, M. Lukowiak, S. Radziszowski, and C. Wood, "Statistical Analysis and Modeling of a Tree-Based Group Key Distribution Method in Tactical Wireless Networks," *submitted to the IEEE Transactions on Wireless Communications*.

J-4. M. Lukowiak, S. Radziszowski, J. Vallino, C. Wood, "Cybersecurity Education: Bridging the Gap between Hardware and Software Domains," *submitted to the IEEE Transactions on Education*.

Conference Proceedings

C-1. 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-2. C. A. Wood, "Chaos-Based Symmetric Key Cryptosystems," In *Proceedings of the 2011 International Conference on Security & Management*, Las Vegas, Nevada. July 2011.

C-3. 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.

Conference Presentations

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

P-2. "Layered Driver Rootkit Detection on Microsoft Windows PCs," Poster Presentation,
RIT Undergraduate Symposium, Rochester Institute of Technology, Rochester, NY. August 24, 2009.

Research Experience

- **Keyboard Biometric-Based Continuous Authentication Schemes**   RIT
  Intelligent Security Systems, Machine Learning   *September 2012 - present*
  - *Advisor:* Dr. Leonid Reznik (CS)
  - I am implementing a real-time keylogger, feature extraction, and classifier engine for use in continuous authentication schemes. Part of the work includes comparing classifiers based on free-form text input against those based on structured text-input. Results are being compared with past and present keyboard-based biometric authentication schemes.

- **Secure Logging Schemes for Cloud-Based SaaS Architectures**   RIT
  Cryptography, Computer Security, Secure Software Design   *July 2012 - present*
  - *Advisors:* Dr. Rajendra K. Raj (CS) and Dr. Andy Meneely (SE)
  - I am developing a novel secure logging architecture for cloud-based SaaS applications that utilizes ciphertext-policy attribute based encryption (CP-ABE) for log file integrity.

- **Wireless Ad-hoc Network Group Key Management**   RIT
  Applied Cryptography, Wireless Networking   *May 2011 - present*
  - *Advisors:* Dr. Stanisław Radziszowski (CS), Dr. Marcin Lukowiak (CE), Dr. Piotr Bajorski (Statistics)
  - Resulted in publication J-3.
  - We are focusing on group key management protocols for wireless ad-hoc radio networks with constrained channel bandwidths and computational power. We explore solutions based on public- and private-key cryptosystems with varying levels of pre-placed radio data for node authentication and key generation. Our work involves implementing network simulators in SMURPH/SIDE and NS3 to obtain empirical performance measurements. We have also developed a mathematical model to compare with quantitative performance metrics.

- $L(2,1)$-**Labeling Problem**   RIT
  Computational Graph Theory   *September 2011 - September 2012*
  - *Advisor:* Dr. Jobby Jacob (Mathematics)
  - Resulted in publications J-1 and J-2 and presentation P-1.
  - I worked on developing a characterization of $L(2,1)$ spans of trees based on their structural properties. As part of this work I implemented a dynamic programming labeling algorithm to assist in the study of tree characterization, which helped to develop tree construction algorithms that are capable of producing infinitely many trees T with a label span of $(\Delta(T) + 2)$. With this, we found a complete $L(2,1)$ label span characterization of trees. We also briefly investigated the $L(2,1)$-labeling problem on cubic bipartite graphs.

- **Secure Operating System Design Principles**   RIT
  Computer Security, Operating Systems   *March 2011 - June 2011*

- *Advisor:* Dr. Rajendra K. Raj (CS)
- I researched secure operating system design principles at all levels of the software stack. The main deliverable was a case study for a variety of popular operating systems with different purposes, including Microsoft Singularity, Chrome OS, Android (the entire stack), QNX, and Microsoft Azure.

- **Rootkit Design, Implementation, and Detection** RIT
  Computer Security, Operating Systems, Malware Design and Detection May 2007 – Aug. 2007
  - *Advisor:* Dr. Rajendra K. Raj (CS)
  - Resulted in publication C-3 and presentation P-2.
  - I examined malware rootkits that targeted the Windows NT family of operating systems. This study included user-mode and kernel-mode rootkit implementations and state-of-the-art static and dynamic techniques. As part of this work I developed a Windows NT filter driver in C to help determine the presence of keystroke-monitoring malware (targeted towards a specific rootkit implementation).

Professional Experience

- **Intel Corporation, Virtual & Parallel Computing Group** Folsom, CA
  Graphics Software Engineer Intern June 2012 - August 2012
  - 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** Victor, NY
  Software Engineer Intern March 2011 - August 2011
  - Designed and implemented a library and supporting drivers for the u-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 an existing CPLD design used to control the power supply in an embedded system.

- **Rochester Software Associates** Rochester, NY
  Software Engineer Intern November 2010 - March 2011
  - 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** Liverpool, NY
  Software Engineer Intern May 2010 - August 2010
  - 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.

Teaching & Other Academic Experience

- **Hardware and Software Design with Cryptographic Applications** RIT
  Teaching Assistant and Lecturer for Dr. Marcin Lukowiak (CE) February 2011 - present

- Developed and delivered lecture material on real-time and embedded software optimization techniques and the Impulse C high-level synthesis tool.
- Assisted students with weekly assignments and graded lab and project deliverables.
- Currently porting the AES cache timing attack on a Xilinx ML507 platform with MicroBlaze soft-core processor for student labs.

- **Computer Science I, II, and IV**   RIT
  Student Lab Assistant and Grader   *January 2009 - present*
  - Proctor weekly problem solving sessions and run lab meetings with brief lectures to cover weekly material.
  - Hold four tutoring office hours per week to assist students in need.
  - Grade weekly lab assignments and midterm examinations.

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

- **Engineering of Software Subsystems**   RIT
  Teaching Assistant for Dr. James Vallino (SE)   *September 2011 - December 2011*
  - 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.
  - Graded course project implementations unit questions.

Honors & Awards

RIT Honors Program . . . . 2009 – present
RIT Tau Beta Pi Engineering Honors Society, member . . . . 2010 – present
Recipient of Golisano College Honors research assistantship award . . . . Spring 2011
Recipient of Golisano College Honors research assistantship award . . . . Winter 2009/2010
Recipient of RIT undergraduate research award stipend . . . . Summer 2009
RIT Golisano College Dean's List . . . . 2008 – present
Student mentor for the FIRST LEGO League team hosted by RIT . . . Fall 2009 – winter 2010

Technical Skills

- Programming Languages: C/C++, C#, Java, Javascript, Python, Ruby, Assembly (MIPS), Scheme
- Modeling Languages and Tools: VHDL, Verilog, UML, SPIN (with PROMELA), Alloy
- Specialized Software: Mathematica, MATLAB, R, Weka
- Markup Languages: LaTeX, HTML, CSS

Personal Information

- Lake Placid Marathon finisher, June 12, 2011. Time of 4:28:08.