CURRICULUM VITAE

NAME: Dr. Benjamin Mood
bmood@pointloma.edu

CURRENT: Professor of Computer Science, Point Loma Nazarene University

GRADUATE AND UNDERGRADUATE SCHOOLS ATTENDED:

University of Florida, Gainesville, Florida, Spring 2014 - Spring 2016
University of Oregon, Eugene, Oregon, Fall 2010 - Summer 2014
Point Loma Nazarene University, Point Loma, California, Fall 2006 - Spring 2010

DEGREES AWARDED:

Doctor of Philosophy, Computer Science, 2016, University of Florida
Master of Science, Computer & Information Science, 2012, University of Oregon Bachelor of Science, Computer Science, 2010, Point Loma Nazarene University

AREAS OF SPECIAL INTEREST:

Security
Compilers and Programming Languages
Game Development
Cryptography

PROFESSIONAL EXPERIENCE:

Teaching at PLNU:

CSC154 – Java II (Object oriented programming)
CSC254/CSC252 – Data structures
CSC323 – Software Engineering
CSC394 – Programming Languages
CSC412 – Special Topics in Computer Science (game design)
CSC493 – Software Project
CSC495 – Service Learning
ISS373 – Networking and Security
ISS403 – Information and Computer Security
CIT324 – Computer and Information Security

Research Assistant:

Fall 2014 - Spring 2016, University of Florida Summer
2011 - Summer 2014, University of Oregon

Research with Kevin Butler for my Masters thesis and PhD dissertation for the advancement of secure computation on mobile devices by improving compilers, execution systems, and developing new and innovative protocols. I am responsible for creating collaborations, developing research ideas, and executing those ideas.

Teaching Assistant: Fall 2010 - Spring 2011, University of Oregon Classes:

Java Programming II (CIS211)
Java Programming I (CIS210)
Intro to the Science of Computing (CIS170)

Responsibilities:

I was responsible for creating and giving lectures in the lab, holding office hours, ad- dressing concerns of the students, and grading assignments for the students.

Adjunct: Summer 2010, Point Loma Nazarene University Class:

Java Programming II (CSC154)

Responsibilities:

I was responsible for creating and giving lectures, creating and grading assignments, creating and grading labs, and holding office hours.

Teaching Assistant: Point Loma Nazarene University, Fall 2008 - Spring 2010 Classes:

Java Programming II (CSC154)
Java Programming I (CSC142)
Datastructures and Algorithms (CSC254)

Responsibilities:

I was responsible for helping students in the lab, holding lab (office) hours, addressing and bringing concerns of the students to the instructor, and grading assignments for the students.

Summer Researcher: Point Loma Nazarene University, Summer 2008

I was responsible to creating a Bayesian network to move a robot around a maze in both Matlab and in C++. I tried different decision algorithms to determine what was the most effective. I used this research as a launching point for my honors thesis; designing a Bayesian network to play rook.

ACTIVE RESEARCH PROJECTS:

Human Perceptions of Violence in Video Games – Summer 2017 – present

Often games are described to be violent or non-violent, but little research has been done on why we perceive certain games in certain ways. In this research, we examine what elements humans perceive violent.

Secure Multiparty Computation with SGX - Spring 2015 - Present

The software guard instruction set (SGX) is a novel instruction set for future Intel processors that will allow programs and data to be separated, by the hardware, from the remainder of the programs and data – securing private data. In this work we examine ways to use SGX to further the efficiency of secure computation. We examine the trust models of SGX and secure computation and present a way to attain the security guarantees of secure computation by using SGX.

INVITED TALKS:

A Practical Mechanism to Perform Secure Computation. ACMS 2017.
Optimizing Garbled Circuit Secure Computation for Mobile Devices, Yale University, 2015
Privacy Preserving Computation on Mobile Devices, Oregon Bioscience Association, 2013
Optimizing Secure Function Evaluation for Mobile Devices, Galois Inc., 2012

GRANTS, AWARDS, AND HONORS:

Gartner Group Graduate Fellowship Endowment, 2014 Travel
Grant, Computer and Communications Security 2014
Research Assistantship, University of Florida, Fall 2014 to Present.
Graduate Research Fellowship, University of Oregon, Summer 2011 to Summer 2014
Erwin and Gertrude Juilfs Scholarship, University of Oregon, Fall 2013
Travel Grant, USENIX Security 2012
Graduate Teaching Fellowship, University of Oregon, Fall 2010 to Spring 2011
Completion of Honors Thesis, Point Loma Nazarene University, Spring 2010

OTHER:

Advanced To Candidacy Spring 2015, University of Florida

Co-founder and co-leader of Graduate Student Bible study at the University of Oregon, Fall 2012 - Spring 2014

Participated in "Downtown Clean-Up" in Downtown Gainesville, August 2015

Helped organize Security Day 2012, 2013, and 2014 at the University of Oregon.

Wrote summaries of presentations for Financial Cryptography and Data Security 2012 and the USENIX Security Symposium 2012.

Sole creator and developer of flash game “Forge’d Cannon”, Spring 2013 – Spring 2016

PUBLICATIONS:

Benjamin Mood and Kevin Butler. PAL: A Pseudo Assembly Language for Optimizing Secure Function Evaluation in Mobile Devices. Journal of Information Security and Applications, 40, pg. 78-91, Jun. 2018.

Henry Carter, Benjamin Mood, Patrick Traynor, Kevin Butler. Outsourcing Secure Two-Party Computation as a Black Box. Journal of Security and Communication Networks (SCN), 2016.

Henry Carter, Benjamin Mood, Patrick Traynor, K. Butler. Secure Outsourced Garbled Circuit Evaluation for Mobile Devices. Journal of Computer Security (JCS), 24(2):137-180, 2016.

Benjamin Mood, Debayan Gupta, Henry Carter, Kevin Butler, and Patrick Traynor. Frigate: A Validated, Extensible, and Efficient Compiler and Interpreter for Secure Computation, Proceedings of the 1st IEEE European Symposium on Security and Privacy, 2016

Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Outsourcing Secure Two-Party Computation as a Black Box, Proceedings of the International Conference on Cryptology and Network Security (CANS), December 2015.

Benjamin Mood, Debayan Gupta, Kevin Butler, and Joan Feigenbaum. Reuse It Or Lose It: More Efficient Secure Computation Through Reuse of Encrypted Values. In Proceedings of the 21st ACM Conference on Computer and Communications Security, Scottsdale, Arizona, November 2014.

Adam Bates, Benjamin Mood, Joe Pletcher, Hannah Pruse, Masoud Valafar, and Kevin Butler. On Detecting Co-Resident Cloud Instances Using Network Flow Watermarking Techniques. International Journal of Information Security: Volume 13, Issue 2, pg. 171-189. 2014.

Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Secure Outsourced Garbled Circuit Evaluation for Mobile Devices 22nd USENIX Security Symposium, Washington, DC, USA, August 2013.

Benjamin Kreuter, ahbi shelat, Benjamin Mood, and Kevin Butler. PCF: A Portable Circuit Format For Scalable Two-Party Secure Computation. 22nd USENIX Security Symposium, Washington, DC, USA, August 2013.

Adam Bates, Benjamin Mood, Masoud Valafar, and Kevin Butler. Towards Secure Provenance-based Access Control in Cloud Environments. 3rd ACM Conference on Data and Application Security and Privacy. San Antonio, TX, USA, 2013.

Benjamin Mood. Optimizing Secure Function Evaluation on Mobile Devices. Masters Thesis, University of Oregon 2012

Benjamin Mood, Lara Letaw, and Kevin Butler. Memory-Efficient Garbled Circuit Generation for Mobile Devices. In *Financial Cryptography and Data Security*, February 2012.

POSTERS:

The Frigate Compiler for Secure Computation, USENIX Security Symposium 2015, Washington D.C.

More Efficient Secure Computation Through Reuse of Encrypted Values, Graduate Student Research Day 2014, University of Florida

Saving Sate in Privacy Preserving Computation, Graduate Research Forum 2014, University of Oregon

Outsourcing Two-Party Privacy-Preserving Computation, Graduate Research Forum 2013, University of Oregon

Privacy Preserving Computations on Smartphones, Graduate Research Forum 2012, University of Oregon

Secure Function Evaluation in Mobile Environments, Department Poster Contest 2011, University of Oregon

CONFERENCE REVIEWS:

Privacy Enchancing Technology Symposium (PETS) 2014 and 2015 USENIX
Security Symposium 2014 and 2015
European Symposium on Research in Computer Security (ESORICS) 2012 and 2014
ACM Conference on Computer and Communications Security (CCS) 2013, 2014, and 2015

JOURNAL REVIEWS:

Transactions on Parallel and Distributed Systems 2017
Transactions on Information Forensics & Security 2017 and 2018
ACM Transactions on Privacy and Security 2017