

## Henry Lee Carter

---

### CONTACT INFORMATION

Assistant Professor  
Villanova University  
Department of Computing Sciences  
800 E. Lancaster Avenue  
Villanova, PA 19085

*Phone:* 610-519-5412  
*E-mail:*  
henry.carter@villanova.edu  
*WWW:* www.henrycarter.org

### RESEARCH INTERESTS

**Developing efficient secure multiparty computation protocols for mobile applications:** applied cryptography, secure mobile applications, privacy-preserving computation

### EDUCATION

**Georgia Institute of Technology**, Atlanta, GA

Ph.D., Computer Science, December 2015

- Advisor: Professor Patrick Traynor
- Dissertation: Efficient Techniques for Secure Multiparty Computation on Mobile Devices

M.S., Computer Science, December 2012

- Specialization: Information Security
- Project Title: *Efficient Mobile Oblivious Computation (EMOC)*

**Belmont University**, Nashville, TN

B.S., Computer Science, May 2010

- *Summa cum Laude*, GPA 3.99
- Minors in Mathematics and Classical Piano

### REFEREED JOURNAL PUBLICATIONS

- [1] N. Scaife, P. Traynor, H. Carter, L. Lidsky, R. Jones. **OnionDNS: A Seizure-Resistant Top-Level Domain.** *International Journal of Information Security (IJIS)*, to appear 2018.
- [2] H. Carter and P. Traynor. **Outsourcing Computation for Private Function Evaluation.** *International Journal of Information and Computer Security (IJICS)*, to appear 2017.
- [3] H. Carter, B. Mood, P. Traynor, K. Butler. **Outsourcing Secure Two-Party Computation as a Black Box.** *Journal of Security and Communication Networks (SCN)*, 9(14):2261-2275, 2016.
- [4] H. Carter, B. Mood, P. Traynor, K. Butler. **Secure Outsourced Garbled Circuit Evaluation for Mobile Devices.** *Journal of Computer Security (JCS)*, 24(2):137-180, 2016.
- [5] H. Carter, C. Amrutkar, I. Dacosta, P. Traynor. **For Your Phone Only: Custom Protocols for Efficient Secure Function Evaluation on Mobile Devices.** *Journal of Security and Communication Networks (SCN)*, 7(7):1165-1176, 2014.

### CONFERENCE PUBLICATIONS

- [6] S. Heuser, B. Reaves, P. Pendyala, H. Carter, A. Dmitrienko, W. Enck, N. Kiyavash, A. Sadeghi, P. Traynor. **Phonion: Practical Protection of Metadata in Telephony Networks.** *Proceedings on Privacy Enhancing Technologies (PoPETs)*, July 2017.

- [7] N. Scaife, H. Carter, P. Traynor, K. Butler. **CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data** *Proceedings of the IEEE International Conference on Distributed Computing Systems (ICDCS)*, June 2016. (acceptance rate: 17.6%)
- [8] B. Mood, D. Gupta, H. Carter, K. Butler, P. Traynor. **Frigate: A Validated, Extensible, and Efficient Compiler and Interpreter for Secure Computation.** *Proceedings of the IEEE European Symposium on Security and Privacy (Euro S&P)*, March 2016. (acceptance rate: 17.3%)
- [9] H. Carter, B. Mood, P. Traynor, K. Butler. **Outsourcing Secure Two-Party Computation as a Black Box.** *Proceedings of the International Conference on Cryptology and Network Security (CANS)*, December 2015. (acceptance rate: 52.9%)
- [10] N. Scaife, H. Carter, P. Traynor. **OnionDNS: A Seizure-Resistant Top-Level Domain.** *Proceedings of the IEEE Conference on Communications and Network Security (CNS)*, September 2015. (acceptance rate: 28.1%)
- [11] B. Reaves, E. Shernan, A. Bates, H. Carter, P. Traynor. **Boxed Out: Blocking Cellular Interconnect Bypass Fraud at the Network Edge.** *Proceedings of the USENIX Security Symposium (SECURITY)*, August 2015. (acceptance rate: 15.7%)
- [12] E. Shernan, H. Carter, D. Tian, P. Traynor, K. Butler. **More Guidelines Than Rules: CSRF Vulnerabilities from Noncompliant OAuth 2.0 Implementations.** *Proceedings of the International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA)*, July 2015. (acceptance rate: 22.7%)
- [13] H. Carter, C. Lever, P. Traynor. **Whitewash: Outsourcing Garbled Circuit Generation for Mobile Devices.** *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, December 2014. (acceptance rate: 19.9%)
- [14] H. Carter, B. Mood, P. Traynor, K. Butler. **Secure Outsourced Garbled Circuit Evaluation for Mobile Devices.** *Proceedings of the USENIX Security Symposium (SECURITY)*, August 2013. (acceptance rate: 16.2%)
- [15] P. Marquardt, A. Verma, H. Carter, P. Traynor. **(sp)iPhone: Decoding Vibrations from Nearby Keyboards Using Mobile Phone Accelerometers.** *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, October 2011. (acceptance rate: 13.9%)
- [16] H. Carter and R. Bhandari, **Improved Sliding Shortest Path Algorithm: Performance Analysis.** *Proceedings of the Southeastern International Conference on Combinatorics, Graph Theory, and Computing (Congressus Numerantium)*, 207:69-81, March 2011.
- WORKSHOP PUBLICATIONS [17] S. Deshmukh, H. Carter, G. Hernandez, P. Traynor, K. Butler. **Efficient and Secure Template Blinding for Biometric Authentication.** *Proceedings of the IEEE Workshop on Security and Privacy in the Cloud (SPC)*, October 2016. (acceptance rate: 40.9%)

UNDERGRADUATE RESEARCH **Belmont University**, Nashville, TN

- Glenn Acree, advisor
- Collegiate CA: designed a certificate authority system and governing policy to be scalable to fit any small college network. (honors thesis, Fall 2008 - Spring 2010)

- WormAnalyzer: developed biology video analysis software implemented in Java. (Spring 2007 - Spring 2008)

TEACHING  
EXPERIENCE

**Villanova University**, Villanova, PA

*Instructor of record*

- CSC 1052: Algorithms & Data Structures II (Spring 2017, Fall 2017)
- CSC 1700: Analysis of Algorithms (Fall 2016)
- CSC 4900: Computer Networks (Fall 2017)
- CSC 5930/9010: Special Topics Cloud Security & Privacy (Spring 2017)
- CSC 8301: Design & Analysis of Algorithms (Fall 2016)
- CSC 8560: Computer Networks (Fall 2017)

**Georgia Institute of Technology**, Atlanta, GA

*Instructor of record*

- CS 4235: Intro to Information Security (Summer 2013)

*Co-instructor*

- CS 8803: Cellular and Mobile Network Security (Fall 2012)

*Guest Lecturer*

- CS 6262: Network Security (Spring 2013-Spring 2015)

**Belmont University**, Nashville, TN

*Teaching Assistant*

- Peer Tutor for CSC 1020: Introduction to Computer Science (Fall 2008)

*Tutoring*

- Math and Computer Science tutor (Fall 2008 - Spring 2010)

GRANTS

**Peer-Reviewed Grants**

- Solderitsch, J., Kim, E., Carter, H., Chasaki, D., Nataraj, C., Grant, “MRI: Acquisition of Scalable Machine Learning Instrumentation for Cybersecurity Research”, NSF, Federal, \$529,108.00, Currently Revising. (sub: January 11, 2017, not funded).

PRESENTATIONS

**Research Talks & Invited Lectures**

- NALS of Philadelphia Saturday CLE, Philadelphia, March 2017, “Cloud Computing: It’s a Fly Ball”
- New Jersey Institute of Technology Computer Science Department Seminar, Newark, October 2016. “Improving biometric authentication with Cloud-based SMC”
- Microsoft Research Workshop on Applied Multi-Party Computation, Redmond, February 2014. “Whitewash: Outsourcing Garbled Circuit Generation for Mobile Devices”
- ISOC Network & Distributed System Security Symposium, San Diego, February 2013. Rump session talk entitled “Outsourcing Secure Function Evaluation: set it and forget it!”
- Belmont Undergraduate Research Symposium, Belmont University, Spring 2010. Presented the Collegiate Certificate Authority system structure and policy.
- Alpha Chi Honors Society National Convention, Indianapolis, IN, Spring 2009. Presented the Collegiate Certificate Authority project concept.

### Refereed Poster Presentations

- USENIX Security Symposium, Washington D.C., August 2015. Poster session presentation entitled “Outsourcing Secure Two-Party Computation as a Black Box”
- ISOC Network & Distributed System Security Symposium, San Diego, February 2015. Poster session presentation entitled “Outsourcing Secure Two-Party Computation as a Black Box”
- USENIX Security Symposium, San Francisco, August 2011. Poster session presentation on Efficient Mobile Oblivious Computation (EMOC) research

### PROFESSIONAL SERVICE

#### Program Committee Member

- ACM SIGCSE Technical Symposium (SIGCSE): 2018
- Annual Computer Security Applications Conference (ACSAC): 2014, 2015
- International Conference on Cryptology and Network Security (CANS): 2016

#### Journal Reviewer

- ACM Transactions on Internet Technology (ToIT): 2016
- ACM Computing Surveys (CSUR): 2016
- Elsevier Computers & Security (COSE): 2016, 2017
- IEEE Transactions on Parallel and Distributed Systems, Trust, Security, & Privacy special issue (TPDS) 25(2): 2014
- Wiley Journal of Security and Communication Networks (SCN): 2016

#### External Conference Reviewer

- ACM Conference on Computer and Communications Security (CCS): 2013, 2015
- ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec): 2016
- ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM): 2012, 2013
- Annual Computer Security Applications Conference (ACSAC): 2012
- IEEE Symposium on Security & Privacy (S&P): 2013, 2014, 2016
- IEEE European Symposium on Security & Privacy (Euro S&P): 2016
- IFCA Financial Cryptography and Data Security (FC): 2013, 2017
- The International Symposium on Research in Attacks, Intrusions and Defenses (RAID): 2015
- ISOC Network and Distributed System Security Symposium (NDSS): 2013, 2014, 2015, 2016
- Privacy Enhancing Technologies Symposium (PETS): 2015
- USENIX Security Symposium (SECURITY): 2013, 2014, 2015, 2016, 2017
- USENIX Workshop on Offensive Technologies (WOOT): 2016

### PROFESSIONAL EXPERIENCE

#### Villanova University, Villanova, PA

*Assistant Professor*

**August 2016 to present**

- Teaching undergraduate and graduate courses in the Computing Sciences department and conducting research in cybersecurity.

#### University of Florida, Gainesville, FL

*Postdoctoral Researcher*

**January 2016 to July 2016**

- Performed research in mobile security and privacy as a part of the Florida Institute for Cyber Security (FICS).

#### Sandia National Laboratories, Albuquerque, NM

*Center for Cyber Defenders Intern*

**May 2011 to August 2011**

- Performed research in collaborative spectrum sensing for cognitive radios. Developed a distributed sensing system with authentication security and robustness to erroneous or imperfect sensing data.

**National Security Agency**, College Park, MD

*Computer Science Internship Program Intern* **May 2010 to August 2010**

- Performed research at the Laboratory for Telecommunications Sciences (LTS) at the University of Maryland.
  - Developed software [Perl] for encoding and transmitting information across delay-tolerant networks using the open-source dtn protocol implementation DTN2
  - Programmed and tested graph algorithms in Matlab for routing network traffic. Statistically demonstrated algorithm improvement over previous existing versions.

**The Nexus Group**, Nashville, TN

*Security Intern* **January 2009 to May 2009**

- A professional internship in information security. The main job task was formulating and documenting company security policies in preparation for an upcoming security audit. Frank Platt, supervisor.

PROFESSIONAL  
MEMBERSHIPS  
SERVICE

Association for Computing Machinery, professional member

Villanova University

- Cybersecurity Program Development Committee, co-chair, Fall 2016-present

Computing Sciences Department, Villanova University

- Department liaison to computer engineering, Fall 2016-present
- BSCS Curriculum Committee, Fall 2016-present
- Colloquium Committee, Fall 2016-present
- CS4ALL Committee, Fall 2016-present
- Diversity Committee, Fall 2016-present
- Faculty Search Committee, Fall 2016-present
- Outreach Committee, Fall 2016-present
- Undergraduate Activities Committee, Fall 2016-present
- Upsilon Pi Epsilon Honors Society advisor, Fall 2017-present

Florida Institute for Cybersecurity Research (FICS), University of Florida

- Lead graduate student, Fall 2014-Spring 2015

Converging Infrastructure Security Lab (CISEC), Georgia Institute of Technology

- Lead graduate student, Fall 2013-Spring 2014

Graduate Student Council, Georgia Institute of Technology

- Student representative, PhD Admissions, 2012
- Social chair, Fall 2010-Fall 2011
- Student coordinator, College of Computing PhD recruitment weekend, Spring 2011

SOFTWARE SKILLS Computer Programming:

- Java, MATLAB, Python, C/C++, Perl, UNIX shell scripting

Version Control and Software Configuration Management:

- Git, SVN

Productivity Applications:

- T<sub>E</sub>X (L<sup>A</sup>T<sub>E</sub>X, B<sub>I</sub>B<sub>T</sub>E<sub>X</sub>), Vim, most common productivity packages (for Windows, OS X, and Linux platforms)

Operating Systems:

- Apple OS X, Linux, Microsoft Windows family

AWARDS

Student Travel Grants

- USENIX Security Symposium, 2015
- Annual Computer Security Applications Conference, 2014
- ACM Conference on Computer and Communications Security, 2013
- ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, 2012
- USENIX Security Symposium, 2011

Nashville Technology Council

- I.T. Student of the Year, 2009

Belmont University

- Raymond H. Medley, Jr. Outstanding Senior Award in Computer Science, 2010
- Belmont University-wide Hale Leadership award for excellence in academics and leadership, 2009 & 2010
- Alpha Chi Honors Society, inducted 2009
- John Von Neumann freshman award for excellence in math and computer science, 2007