# Paul Vines

**Phone: (703)284-8458** **Clearance: SECRET**

**E-Mail: paul.l.vines@gmail.com** **Website: paulvines.com**

## Summary

Cybersecurity researcher with experience in formal methods, machine learning, and network security and privacy. Interested in performing research focused on advancing the state-of-the-art in cybersecurity to provide resilience and automation. Other research interests include anonymity, privacy, network security, and adversarial machine learning.

## Education

**Ph.D.** **2017**
Allen School of Computer Science & Engineering, University of Washington, Seattle, WA

**Master of Science** **2015**
Allen School of Computer Science & Engineering, University of Washington, Seattle, WA

**Bachelor of Science** **2012**
*Valedictorian;* Computer Science and Biology, Roanoke College, Salem, VA

## Experience

**Senior Principal Research Engineer – FAST Labs / BAE Systems Inc.** **2017-Present**
- Principal Investigator on DARPA SafeDocs developing verified input parsers
- Lead development of Network Tomography Inference on DARPA EdgeCT
- Developed novel research proposals for formal program verification and software safety assurance
- Explored quantification and propagation of confidence in software safety assurance cases
- Investigated ML classification of encrypted multiplexed network traffic

**Graduate Researcher – University of Washington** **2012-2017**
- Pioneered using targeted advertising for personal surveillance (ADINT)
- Developed and used the Checker Framework to detect Android malware via information flow type analysis as part of DARPA APAC
- Extended Checker Framework to support resolution of Reflection
- Evaluated web-tracking and user privacy defense efficacy using machine learning
- Designed and implemented a covert communication system utilizing game network traffic

**Software Engineer - ExtraHop Networks** **Mar-Jun 2015**
- Wrote high-performance C code to process and analyze network traffic
- Engaged in team software development on a large multi-component project

**Security Engineer – NCC Group** **Jun-Sep 2013**
- Constructed and programmed a PIN-cracking robot
- Investigated ZigBee home alarm system security

## Skills

- Computer and Network Security
- Technical Writing and Communication
- Experience with static analysis and full program verification tools (ACL2, Coq, Dafny)
- System Design, Threat Modeling, and Implementation
- Reverse Engineering of X86 Binaries and Network Protocols
- Experience Programming in: Python, CommonLisp, Java, C, JavaScript, Elm
- Training in formal methods in programming languages at OPLSS 2019 and graduate coursework
- Data Analysis and Visualization
- Cloud/Docker-based webcrawling infrastructure creation

## Publications

- Reasoning with Assurance Arguments Under Uncertainty. Sumit Ray, Rebecca Cathey, Paul Vines, Allyson O'Brien
- Exploring ADINT Exploring ADINT: Using Ad Targeting for Surveillance on a Budget — or — How Alice Can Buy Ads to Track Bob. Paul Vines, Franziska Roesner, Tadayoshi Kohno. WPES 2017
- Rook: Using Video Games as a Low-Bandwidth Censorship Resistant Communication Platform. Paul Vines, Tadayoshi Kohno. WPES 2015
- Static Analysis of Implicit Control Flow: Resolving Java Reflection and Android Intents. Paulo Barros, Rene Just, Suzanne Millstein, Paul Vines, Werner Dietl, Marcelo D'Amorim, Michael D. Ernst. ASE 2015
- Collaborative Verification of Information Flow for a High-Assurance App Store. Michael D. Ernst, Rene Just,
  Suzanne Millstein, Werner Dietl, Stuart Pernsteiner, Franziska Roesner, Karl Koscher, Paulo Barros, Ravi Bhoraskar, Seungyop Han, Paul Vines, Edward X. Wu. CCS 2014
- R2B2: PIN-Cracking Robot. Justin Engler, Paul Vines. DefCon 2013.