Stacy J. Prowell

Director
Vehicle Security Center
Oak Ridge National Laboratory

Program Manager
Cybersecurity for Energy Delivery Systems (CEDS)
Sustainable Electricity Program
Oak Ridge National Laboratory

Chief Cyber Security Research Scientist
Computational Science and Engineering Division
Oak Ridge National Laboratory

Cyber Warfare Research Team Leader
Cyber and Information Security Research Group
Oak Ridge National Laboratory

Associate Professor (Joint Appointment with ORNL)
Department of Electrical Engineering and Computer Science
The University of Tennessee, Knoxville

WORK

One Bethel Valley Rd
PO Box 2008, MS-6418
Oak Ridge, TN 37831-6418, USA

+1 (865) 241-8874 (voice)
+1 (865) 576-5943 (fax)

prowellsj@ornl.gov

US Citizen

HOME

1165 Gilbert Station Ln
Knoxville, TN 37932, USA

+1 (724) 307-8229 (mobile)

sprowell@gmail.com

Current Research

- Computationally-intensive methods in cyber security and software engineering
- Deep inspection of compiled software for vulnerability detection and software assurance
- Microelectronics assurance using advanced imaging techniques

Experience

November 2015 – Present: *Director*, Vehicle Security Center, Oak Ridge National Laboratory

> *Director*: Responsible for strategic direction of center.
> Accomplishments: Created the Vehicle Security Center by combining expertise in vehicle systems, embedded systems, and cyber security, with specialized facilities at the National Transportation Research Center in Knoxville, TN.

August 2013 – Present: *Program Manager*, Cybersecurity for Energy Delivery Systems (CEDS), Sustainable Electricity Program, Oak Ridge National Laboratory. http://web.ornl.gov/sci/eere/sustainable_electricity.shtml

> *Program Manager*: Manage ORNL's portfolio of research efforts for security the nation's energy distribution systems. This program currently consists of a per year basic research investment from the Department of Energy's CEDS program, along with competitively-funded efforts and the lab's own internal investments.

December 2009 – Present: *Chief Cyber Security Research Scientist*, Computational Sciences and Engineering Division, Oak Ridge National Laboratory. http://computing.ornl.gov/cse/index.shtml

> *Chief Cyber Security Research Scientist*: Responsible for development and execution of laboratory strategy and priorities on cyber security. Focus on entrepreneurial development of new programs and growth of existing programs.
>
> *Cyber Warfare Research Team Lead*: Assembled and presently manage a team of 18 researchers in cyber security, focusing on four strategic thrusts: Automated Behavior Computation, Embedded System Security, Developing a National Malware Repository, and Ultra-Secure Communications and Authentication.
>
> - **ORNL Significant Event Award**: Three technologies (Hyperion, Choreographer, and USB-ARM) selected for DHS Transition to Practice (TTP) program. DHS selected eight technologies nationwide for TTP; three came from the Cyber Warfare Research Team.
>
> *Support Efforts:* In order to support the CWR team and CSIIR group research efforts, created specialized facilities within the team.
>
> - **Center for Trustworthy Embedded Systems (CTES)**, Dr. Jason Carter (Director). This is a dedicated laboratory facility with a large Faraday cage, offices, and laboratory space that supports the team's efforts in embedded software for multiple sponsors, including the transportation, military, and medical device communities.

- **Blackbox**, Dr. Stacy Prowell (Director) and Dr. Jeff Nichols (Facility Manager). This is a computing facility that provides multiple cluster computer architectures, elastic cloud computing, network storage, and research networks for use by multiple projects using a simple subscription model.

Principal Investigator:

- **1SR** (2016-Present) – Multiple sponsors. Comprehensive solution for performing network operations training, evaluating alternative network configurations, and deploying untrusted and early-stage cyber security solutions on a network to improve security in a manner that *can not* disrupt the operational network.
- **Cyber Science Laboratory** (anticipated 2017 start) – US Department of Energy. This is a large-scale effort combining eight national laboratories and one test site for ongoing, sustained efforts in cyber security.
- **Transition to Practice – Hyperion** (2012-2014) – US Department of Homeland Security, $300k over two years. Hyperion is commercially licensed and is an R&D 100 Award Winner (November 2015).
- **Legacy** (2012-2014) – Applied Communication Sciences (ACS), $3.2M over two years. Automated computation of legacy software component behavior.
- **Automated Vulnerability Detection (AVUD) Demonstration** (2013-2014) – US Department of Energy, $300k over one year. Demonstrate automated vulnerability detection in a smart meter. Partnership with Sensus USA, Inc.
- **Decision Support Systems Component for DDDAS** (2013-2015) – University of Arizona (for Air Force Office of Scientific Research), $200k.
- **Function Extraction and Executable Decomposition (FEED)** (2012-2013) – Lockheed Martin Federal Systems, $500k over 1 year. Automatically assess the impact of software patches.
- **Beholder: Robust Cyber Event Detection** (2011-2013) – US Department of Energy, $240k over 2 years. Exploit the physics of computation to remotely detect intrusion events in deployed systems. Partnership with General Electric Research.
- **Automated Vulnerability Detection (AVUD) for Compiled Smart Grid Software** (2010-2012) – US Department of Energy, $3M over 2 years.
- **Research, Demonstration, Test and Evaluation Support** (2011-2012) – US Department of Transportation, $220k over 1 year. Project is *ongoing*, but has been handed off to the new Center for Trustworthy Embedded Systems.

- **Ultrascale Algorithms for Verification of Security Properties** (2010-2012) – ORNL internally funded effort, $600k over 2 years.
- **Using Semantic Analysis to Detect and Classify Executables for Computer Forensics** (2010-2012) – US Federal Sponsor, $240k over 2 years.
- **Host Based Malware Detection**, Technology Forecast (2011-2012) – US Federal Sponsor, $120k.
- **Function Extraction Research Support** (2010-2011) – MITRE, $300k.

Co-PI:

- **Research, Development, Technology Assessment, Integration, and Implementation** (2011-Present) – US Army Space and Missile Defense Command.

July 2010 – Present: *Associate Professor* (Dual Appointment with ORNL), Department of Electrical Engineering and Computer Science, The University of Tennessee. http://www.eecs.utk.edu/

Assisted in the development of a curriculum for a Cyber Security Emphasis in the EECS department.

Assisted in the development of a new Ph.D. program in data science offered through UT's Bredesen Center.

Engaged in efforts to create a Center for Cybersecurity Research as a collaborative investment among multiple parties including the University and local and national businesses.

August 2005 – December 2009: *Chief Scientist*, CERT STAR*Lab, Software Engineering Institute, Carnegie Mellon University. http://www.sei.cmu.edu/
Joint Faculty, Information Networking Institute, Carnegie Mellon University. http://www.ini.cmu.edu/

Chief Scientist: CERT STAR*Lab (Security Technology Automation and Research). http://www.cert.org/sse/starlab.html STAR*Lab is a CERT laboratory for developing proof-of-concept automation to solve challenge problems in software security. Projects include: Function Extraction, Computational Security Attributes, Automated Correctness Verification, Automated Component Composition, Flow-Service-Quality Engineering.

Principal Investigator:

- **Automated Structuring for Understanding Legacy Software** – Support analysis of malicious code by automatically determining correct program control flow in the presence of obfuscation.
- **Flow-Service-Quality (FX) Engineering** – Provide abstractions to anchor the specification, development, deployment, and maintenance of large network-centric systems.

- **CTC CAMP Project** – Review of static analysis tools for use by US Gov't.

Team Lead and Architect: Function Extraction (FX) project. Developed software to allow automated analysis of malware by computing the full functional effect of binary code.

April 2004 – August 2005: *Visiting Scientist*, Software Engineering Institute, Carnegie Mellon University. http://sei.cmu.edu

January 1999 – August 2005: *Research Associate Professor*, Department of Computer Science, The University of Tennessee. http://www.utk.edu/

Principal Investigator: Software Assurance for the Spallation Neutron Source (ORNL SNS), $200k over 2 years.

External Collaborator: Feasibility Study of Automated Program Behavior Computation for Next-Generation Software Engineering, $120k over ten months – The Boeing Company.

Manager: Experimentation, Simulation, and Prototyping (ESP) Project, Software Quality Research Laboratory. Created tools to support transfer of testing and specification technologies. Testing tool (JUMBL) is presently in use by 30+ organizations.

Research: Conducted research on requirements engineering and software assurance in collaboration with NORTEL (1999-2004), CTI-PET Systems (1999-2004), Raytheon (2001), and Alpine Engineered Systems (2000).

October 1998 – August 2005: *Adjunct Assistant Professor*, Computer Science, The University of Tennessee. http://www.utk.edu/

May 2004 – December 2011: *Founder and Member*, Software Silver Bullets, LLC. Rigorous model-based automated software testing.

April 2000 – October 2000: *Consultant*, NexWare, Inc. Embedded systems design and implementation, including set-top boxes and internet appliances.

May 1998 – January 1999: *Consultant*, Q-Labs, Inc. Business area development for rigorous methods training, coaching, and tools.

May 1995 – May 1998: *Computer Scientist*, Software Engineering Technology, Inc.

Academic Service

Conferences and Workshops

- General Chair, CISR Conference (April 2016).
- Judge, CodeTN Competition (http://codetn.org, November 2015).
- General Chair, CISR Conference (April 2015).
- Judge, CodeTN Competition (November 2014).
- General Chair, CISR Conference (April 2014).

- Program Co-Chair, 8th Annual CSIIRW (January 2013).
- Minitrack Co-Chair, Dynamic Analysis of Software Systems, HICSS-44 (January 2012).
- Program Co-Chair, 7th Annual CSIIRW (October 2011).
- Minitrack Co-Chair, Assurance Research for Dependable Software Systems, HICSS-43 (January 2011).
- Program committee member on numerous conferences and workshops.

Doctoral Committee Member

- Jarylin Hernández Jiménez (advisor: Katerina Goseva-Popstojanova), Ph.D. Computer Science, expected 2017, West Virginia University.
- Wesley Jin (advisor: Dr. Priya Narasimhan), Ph.D. Computer Science, awarded 2014, Carnegie Mellon University
- Chris Symons (advisor: Dr. Greg Peterson), Ph.D. Computer Science, awarded 2013, The University of Tennessee
- Balajee Kannan (advisor: Dr. Lynne Parker), Ph.D. Computer Science, awarded 2006, The University of Tennessee
- Lan Lin (advisor: Dr. Jesse Poore), Ph.D. Computer Science, awarded 2006

Masters Committee Member

- David Heise (advisor: Dr. Michael Thomason), MS Computer Science 2013, The University of Tennessee
- Carrie Black (co-advisor with Dr. Dawn Song), MS Computer Science, 2006, Carnegie Mellon University
- Carla Sparks, MS Computer Science, 2004, The University of Tennessee
- Damodar Balgi, MS Computer Science, 2004, The University of Tennessee
- Michael Corum, MS Computer Science, 2003, The University of Tennessee
- Michael Campfield, MS Computer Science, 2002, The University of Tennessee
- Jay Patel, MS Computer Science, 2001, The University of Tennessee
- Janet Seib, MS Computer Science, 2001, The University of Tennessee
- David Pearson, MS Computer Science 2001, The University of Tennessee

Open Source Projects

See my open source report card here: https://osrc.dfm.io/sprowell/, assuming OSRC is working. I routinely write solid, scalable, fast code in C, C++, Python, Java, Scala, and sometimes assembly. I am currently working on an HPC project using Rust.

- **Elision**, a fast term rewriter that merges the type and term spaces allowing for higher-level rewriting. See: http://elision.github.com. Elision is used in static analysis of programs, and is written in Scala. A new version is being written in Rust.

- **Pico**, an elastic platform for safe malware handling and malware analysis. See: http://mons-pico.github.com. The Pico encoding and reference are open source; a populated malware platform using HBASE and HADOOP is available at Oak Ridge National Laboratory. There are C, Java, and Python implementations of the Pico encoding.
- **He4** is a fixed-memory, open addressing hash table with linear probing and LRU deletion, designed for embedded applications. See: https://github.com/sprowell/he4
- **SPSPS** is Stacy's Pathetically Simple Parsing System, a tiny framework in vanilla C for writing parsers along with fast mutable and immutable strings and a fast JSON parser. See: http://github.com/sprowell/spsps.

Patents

- S. J. Prowell, "Performing Hierarchical Analysis of Markov Chain Usage Models," US Patent 7,219,049, filed September 15, 2003.
- S. J. Prowell and C. Rathgeb, "Statistical Fingerprinting for Malware Detection and Classification," US Patent 9,135,440, filed July 31, 2013.
- P. Evans, N. Paul, S. Prowell, "System and Method for Key Generation in Security Tokens," US Patent 9,172,698, filed October 11, 2013.
- S. J. Prowell and K. D. Sayre, "Automated Clustering of Malware Variants Based on Structured Control Flow," Provisional Patent #62/170,758, filed June 4, 2015.

Recent Articles

- R. Abercrombie, L. Hively, S. Prowell, B. Schlicher, and F. Sheldon, "Forewarning of Failure in Complex Systems," *Journal of Homeland Security*, v. 5, n. 1, June 2011, pp. 1-16.

- L. Lin, S. Prowell, and J. Poore, "An Axiom System for Sequence-Based Specification," *Theoretical Computer Science*, v. 411, n. 2, February 2010, pp. 360-376.

- L. Lin, S. Prowell, J. Poore, "The Impact of Requirements Changes on Specifications and State Machines," *Software Practice & Experience*, v. 39, n. 6, June 2009, pp. 573-610.

- S. Prowell and J. Poore, "Computing System Reliability Using Markov Chain Usage Models," *Journal of Systems and Software*, v. 73, n. 2, September 2004, pp. 219–225.

- S. Prowell and J. Poore, "Foundations of Sequence-Based Software Specification," *IEEE Transactions on Software Engineering*, v. 29, n. 5, May 2003, pp. 417–429.

Invited Talks

- S. Prowell, Invited Talk: "Security and Privacy for Vehicle Systems and Systems of Vehicles," DHS Automotive Cybersecurity R&D Showcase, Volpe Center, Cambridge, MA, October 17, 2016.

- S. Prowell, Invited Talk: "Vehicle Security," Minnesota State University, Student IEEE Section, Mankato, MN, October 3, 2016.

- S. Prowell, Invited Talk: "Vehicle Security," Southern Minnesota IEEE Chapter, Rochester, MN, October 3, 2016.

- S. Prowell, Invited Talk: "Vehicle Security," Exploring Cybersecurity Challenges in Electrified Transportation: A Focused Workshop (IEEE), Howard University, Washington, DC, February 24, 2016.

- S. Prowell, Keynote Talk: "Security, Verification, and the IoE," Program Protection and Reverse Engineering Workshop (PPREW), Los Angeles, CA, December 8, 2015.

- S. Prowell, Plenary Talk: "Let's Instrument Everything – And Trust It," Future of Instrumentation and the Internet Workshop, Arlington, VA, May 4-6, 2015. On web: http://goo.gl/avgydd (retrieved August 4, 2015).

- S. Prowell, Keynote Talk: "Verification and Security," *Midwest Verification Days*, University of Missouri, October 3-4, 2015.

- S. Prowell, Invited Talk: "Enabling Insecurity: Bringing the Tools and Techniques from IT to Control Systems," TCIPG Lecture Series, University of Illinois, December 6, 2013.
  On web: https://goo.gl/SQ1sIf (retrieved August 4, 2015).

- S. Prowell, Invited Talk and Panelist: Capitol Hill Briefing on "Cybersecurity and Smart Infrastructure," *Science and the Congress Project*, sponsored by the American Chemical Society (ACS), Washington, DC, April 19, 2012.

- S. Prowell, Invited Talk: "Insecurity in Cyberspace," Howard Baker Center, Knoxville, TN, October 19, 2010.

- S. Prowell, Invited Talk: Dagstuhl Seminar 04371, "Perspectives on Model-Based Testing," Germany, September 2004.

Books

- S. Prowell, R. Kraus, M. Borkin, *Seven Deadliest Network Attacks*, Syngress: Boston, MA, 2010.

- S. Prowell, C. Trammell, R. Linger, and J. Poore, *Cleanroom Software Engineering: Technology and Process*, Addison-Wesley: Boston, MA, 1999.

Chapter and Reports

- J. Hernandez, L. Hively, E. Downing, A. Ferber, S. Prowell, R. Wagner, "Beholder: Phase-Space Detection of Cyber Events," ORNL Technical Report ORNL/TM-2013/294, 2013.

- N. Paul, L. Hively, S. Prowell, "Host-Based Malware Detection," (awaiting distribution), ORNL Technical Report ORNL/TM-2013/231, 2013.

- A. Hevner, R. Linger, M. Pleszkoch, S. Prowell, G. Walton, "Flow-Service-Quality (FSQ) Systems Engineering: A Discipline for Developing Network-Centric Information Systems," *Systems Analysis and Design: Techniques, Methodologies, Approaches, and Architectures*, R. Chiang, K. Siau, and B. Hardgrave, eds., M. E. Sharpe: New York, NY, April 2009.

- A. Hevner, R. Linger, R. Collins, M. Pleszkoch, S. Prowell, and G. Walton. "The Impact of Function Extraction Technology on Next Generation Software Engineering," SEI Technical Report CMU/SEI-2005-TR-015, Software Engineering Institute, 2005.

- S. Prowell and J. Poore, "Reliability Computation for Usage-Based Testing." *Modern Statistical and Mathematical Methods in Reliability* (Volume 10: Series on Quality, Reliability and Engineering Statistics, A. Wilson, N. Limnios, S. Keller-McNulty, and Y. Armijo, eds.). Hackensack, NJ: World Scientific Publishing, 2005.

- R. Linger and S. Prowell, "Developing Secure Software with Cleanroom Software Engineering," *Improving Security Across the Software Development Lifecycle*, (Task Force Report, Volume II, National Cyber Security Summit, S. Redwine and N. Davis, eds.). March 2004.

- S. Prowell, "Computations for Markov Chain Usage Models," UT Technical Report UT-CS-03-505, the University of Tennessee, 2003.

Peer-Reviewed Conference Presentations

- S. Prowell, "One Step Removed (1SR) Concept Overview," *DOE Cyber Conference*, Atlanta, GA, September 19-22, 2016.

- J. M. Hernández, A. Ferber, S. Prowell, L. Hively, "Phase-Space Detection of Cyber Events," *Proc. of the 10th Annual Cyber and Information Security Research (CISR) Conference*, Oak Ridge, TN, April 7-9, 2015.

- J. Stoll, S. Prowell, J. Goodall, R. Stewart, D. White, B. Bhaduri, "GEOINT for Cybersecurity," GEOINT Summit, Washington, DC, June 2013.

- J. Hernández, L. Pouchard, J. McDonald, S. Prowell, "Developing a Power Measurement Framework for Cyber Defense," CSIIR Workshop, Oak Ridge, TN, January 2013.

- R. Linger, M. Pleszkoch, S. Prowell, K. Sayre, and T. Ankrum, "Computing Legacy Software Behavior to Understand Functionality and Security Properties: An IBM/370 Demonstration," CSIIR Workshop, Oak Ridge, TN, January 2013.

- S. Prowell, M. Pleszkoch, K. Sayre, and R. Linger, "Automated Vulnerability Detection for Compiled Smart Grid Software," IEEE PES Innovative Smart Grid Technologies Conference, January 2012.

- R. Linger, M. Pleszkoch, S. Prowell, and K. Sayre, "Behavior Computation for Smart Grid Software Analysis," CSIIR Workshop, Oak Ridge, TN, October 2011.

- R. Abercrombie, L. Hively, S. Prowell, R. Schlicher, and F. Sheldon, "Forewarning of Failure in Complex Systems," DHS Science Conference – 5th Annual University Summit, Washington, DC, April 2011.

- S. Fernandez, S. Prowell, and J. Nutaro, "Behavior-Based Anomaly Detection: Capabilities and Future Directions," CyberCap, Dallas, TX, August 2010.

- R. Bartholomew, L. Burns, T. Daly, R. Linger, and S. Prowell, "Function Extraction: Automated Behavior Computation for Aerospace Software Verification and Certification," AIAA Infotech@Aerospace 2007 Conference, Rohnert Park, CA, May 2007.

- A. Mili, T. Daly, M. Pleszkoch, and S. Prowell, "A Semantic Recognizer Infrastructure for Computing Loop Behavior," 40th Annual Hawaii International Conference on System Sciences (HICSS'40), Kona, HI, January 2007.

- S. Prowell, "Using Markov Chain Usage Models to Test Complex Systems," 38th Annual Hawaii International Conference on System Sciences (HICSS'38), Kona, HI, January 2005.

- F. T. Sheldon, S. G. Batsell, S. J. Prowell, and M. G. Langston, "Position Statement: Methodology to Support Dependable Survivable Cyber-Secure Infrastructures," 38th Annual Hawaii International Conference on System Sciences (HICSS'38), Kona, HI, January 2005.

- S. Prowell and W. T. Swain, "Sequence-Based Software Specification of Critical Software Systems," American Nuclear Society NPIC & HMIT, Columbus, OH, September 2004.

- S. Prowell and J. H. Poore, "Computing System Reliability Using Markov Chain Usage Models," Fourth International Conference on Mathematical Methods in Reliability, Santa Fe, NM, June 2004.

- S. Prowell, "A Cost-Benefit Stopping Criterion for Statistical Testing," 37th Annual Hawaii International Conference on System Sciences (HICSS'37), Kona, HI, January 2004.

Awards and Honors

- Selected as an IEEE Distinguished Lecturer by the Transportation Electrification Community (2016).
- 2016 ORNL Lab Director "Best SEED Money Fund Poster" Award (with Jeff Nichols, Bobby Bridges, and Jarylin Hernández).
- 2016 Federal Laboratory Consortium Excellence in Technology Transfer Award (with David Sims).
- 2015 R&D 100 Award (for Hyperion).
- 2015 UT-Battelle Technology Commercialization Award (for Hyperion Team).
- 2013 UT-Battelle Significant Event Award.
- 1992 Chancellor's Citation for Extraordinary Academic Achievement.

Education

B.S. (1992), M.S. (1995), and Ph.D. (1996), Computer Science, The University of Tennessee. Dissertation: "Sequence-Based Software Specification."

References

Available upon request.