ROBERT E. GILLEN CURRICULUM VITAE

Vulnerability Science
Cyber Resilience and Intelligence
National Security Sciences Directorate
Oak Ridge National Laboratory
P.O. Box 2008, MS-6280
One Bethel Valley Road Oak Ridge, TN 37831-6280 U.S.A.

Phone: 865-341-8121
Email: rob@robgillen.com

Website: http://robgillen.com
LinkedIn: https://www.linkedin.com/in/gillenrob/
ORCID: https://orcid.org/0000-0002-9002-1440
Google Scholar: https://scholar.google.com/citations?user=aWpgGlcAAAAJ
ResearchGate: https://www.researchgate.net/profile/Robert_Gillen2

Areas of specialization

Vulnerability Science • Critical Infrastructure • Machine Learning • Cyber Security • Text Mining • Cloud Computing • Embedded Systems • Digital Forensics

Honors & Awards

2018 IEEE Senior Member
2018 Association of Computing Machinery (ACM) Senior Member
2016 UT-Battelle Community Outreach Award
2016 ORNL Significant Event Award (SEA) (Support for Overseas Testing)
2013-2015 Microsoft MVP: Developer Security
2012 ORNL Significant Event Award (SEA) (for demonstration of zero-day network attack detection)
2010-2012 Microsoft MVP: Windows Azure
2011 ORNL Significant Event Award (SEA) (for support of cyber attack response)
2010 ORNL Recognition for Exceptional Mentoring in the Research Alliance in Math and Science Summer Internship

Professional Experience

2011-present Distinguished Research Staff
Vulnerability Science
Cyber and Applied Data Analytics Division
National Security Sciences Directorate
Oak Ridge National Laboratory, Oak Ridge, TN

My current work is focused on deeply understanding software and systems - both how they work and how they may be exploited for malicious intent. This information is used to then strengthen and fortify those systems and software. To accomplish these objectives, we utilize various research-focused approaches to explore and focus the problem domain.

Previously, my work was focused on helping domain scientists and other government organizations effectively use computational techniques to accomplish their research or mission objectives. I apply techniques from data science, signals processing, cyber security, and industry to address issues of national significance. I both led projects and participate as a team member.

Responsibilities: Conducting research and development at both the Principal Investigator and Investigator levels; establishing and maintaining funding sources; publishing, presenting, and demonstrating to academic, industry, and federal communities; mentoring students and junior research staff; management of equipment acquisition and maintenance; performing professional service activities; recruiting and hiring new employees.

2009-2011 Computer Scientist [Contractor]
Computer Science Research Group
Computer Science and Mathematics Division
Oak Ridge National Laboratory, Oak Ridge, TN
Planet Technologies, Inc., Germantown, MD

While working for CSR, I was directly responsible for analyzing the existing cloud platforms and assessing their suitability for various scientific computational workloads. I met regularly with the leading cloud vendors and consulted with them to merge high-computation demands with the high-availability and fault-tolerant concerns prevalent in industrial cloud designs.

Responsibilities: Conducted research and development into the ways in which cloud computing could be leveraged by the scientific computing community. Worked closely with industry partners (Amazon, Microsoft) to perform testing and develop guidance for scientists regarding the most appropriate ways in which to leverage their platforms. Participated in the Microsoft Azure advisory board and, along with others, provided feedback leading to the broadening of the computational systems offered by that organization.

2007-2009 Senior Solutions Architect [Contractor]
Information Technologies Solutions Division
Oak Ridge National Laboratory, Oak Ridge, TN
Planet Technologies, Inc., Germantown, MD

Sent to ORNL on behalf of Planet Technologies to support in the deployment of various Microsoft-centric solutions across the laboratory. During this time I assisted in systems architecture, knowledge transfer, and hands-on development of a number of the business systems. During this time I also directly participated in supporting a number of

network security efforts and tools allowing their Windows user-base to run with least-user-privilege while still having the flexibility to install software and manage their workstations.

2000-2007 Senior Solutions Architect
Planet Technologies, Inc., Germantown, MD

Lead developer supporting Planet's system integration business. Worked with and often on behalf of Microsoft corporation on many customer engagements. My specialty was automating the provisioning of both shared and dedicated services on top of the Microsoft technology stack and in this role directly supported many international telecommunication companies as they provided Internet services to their customers.

1999-2000 Senior Technical Lead
Conserve-A-Net Internet Services, Independence, MO

Participated in an Internet start-up aimed at providing filtered (parent-limited content) Internet services. In this role, I was responsible for all technology implementations in the organization including web and email servers, routers, firewalls, and dial-up modem banks. Coordinated efforts with up-stream service providers and tier-3 customer service issues. Developed our third-party hosting platforms and assisted customers with migrations.

1998-1999 Network Administrator, Teacher
Tri-City Christian School/Ministries, Blue Springs, MO

At Tri-City, I was responsible for all technical services provided to the organization. This included everything from the network and computing infrastructure to audio/visual equipment. While there, I designed and implemented an upgrade/replacement of the existing network from multiple token-ring segments to a unified Ethernet-based network supporting 10/100 Mbps. This work also involved the implementation of a domain infrastructure and centralized accounts to support the school management system. In addition to general technical responsibilities, I co-taught a computer applications class at the junior/senior high-school level.

1996-1998 Application Developer
The Wilds Conference Center, Brevard, NC

Having worked with the Wilds in a part-time capacity (summer staff) since 1994, I began a more consistent role in building simple software solutions to support their operations while completing my college education. Initially this work involved working with the food services division and purchasing agents to build utilities to track and optimize costs. Later, the work effort focused on automation of the attendee registration and room assignment system which, at that time, was completely manual/paper-based.

Education

2015-2020 PhD in Engineering (focus: Computer Science)
Tennessee Technological University, Cookeville, TN

2015-2018 M.S. in Computer Science
Tennessee Technological University, Cookeville, TN

1994-1998 B.S. in Broadcast Engineering (Minor: Computer Science), *Honors*
Bob Jones University, Greenville, SC

Industry Certifications

2014 Certified Ethical Hacker (CEH)
2013 Offensive Wireless Security Professional (OWSP)
2012 Microsoft Certified Professional (MCP) - Windows Azure
2000 Microsoft Certified Systems Engineer (MCSE), MCPID 1864693
2000 Cisco Certified Network Associate (CCNA)

Technical Skills

Machine Learning • Python • C/C++/C# • ELK • Git • LaTeX • JavaScript/HTML • Matlab • Linux • Cuda • OpenCL • Verilog

Grants & Contracts

Selected Research Grants

2023-2024 *Principal Investigator*, Critical Infrastructure Vulnerability Assessment and Recommendations, $1,000,000
2022-2023 *Investigator*, Black-Box introspection of machine-learning models, Task budget $500,000
2020-2023 *Subject Matter Expert*, Vulnerability Assessments of Critical Infrastructure Devices, Task budget $950,000
2020-2021 *Principal Investigator*, Software/Hardware Vulnerability Assessment of critical infrastructure testing equipment, $750,000
2019-2021 *Principal Investigator*, Software Vulnerability Assessment, $1,790,000
2018-2020 *Principal Investigator*, Developing Red-Team Capabilities for Challenging ML-Based Defenses for Cyber-Physical Systems, $1,395,000
2016-2019 *Principal Investigator*, Analyzing and scaling existing scientific platform to leverage cluster computing and GPU-enabled resources, $1,500,000
2017-2019 *Investigator*, Data Analytics Platform, Task budget $500,000
2018 *Task Lead*, Infrastructure and Computation Support for Software-Defined Counter-UAS System, $30,000
2018 *Principal Investigator*, Studying the use of FPGA-based Neuromorphic Computing Cards

for Cyber Defence, $50,000

2017-2018 *Principal Investigator*, Designed and lead a team building an open-source platform for shared analytics, compute, and data storage $250,000

2011-2018 *Principal Investigator*, Designed and developed a text analysis workbench supporting large-scale text forensics, $4,300,000

2014-2018 *Task Lead*, User interface and integration supporting remote embedded systems, Task funding approximately $1,400,000, total project $5,400,000

2011-2017 *Investigator*, Machine learning system for network traffic classification, engineering and integration, Task funding approximately $600,000, total project, $8,000,000

2014-2017 *Principal Investigator*, Custom embedded systems design/development for signals analysis, $940,000

2014-2016 *Principal Investigator*, Study on developing and using synthetic data supporting data analytics research, $450,000

2012-2014 *Task Lead*, "Knowledge Discovery Infrastructure", Center for Medicare and Medicaid Services (CMS), $1,250,000 ($18M project total)

2009-2011 *Investigator* "Scientific Uses of Cloud Computing", Laboratory Directed Research and Development, $700,000

Commercial Contracts

The items in this section are listed to provide insight into the breadth of experience in the commercial sector prior to transitioning to research. Due to the nature of these contracts, many customer/company names are withheld and contract figures are rounded. Specifics can be provided if necessary

2005 *Lead*, "Provisioning System Solution Architecture and Deployment Support", large ISP, Rome, Italy, $75,000.

2005 *Team Lead*, "Provisioning System Development and Platform Design", mid-sized hosting company, Nottingham, England, $125,000.

2004 *Team Lead*, "Provisioning System Solution Architecture", mid-sized ISP, Amsterdam, NL, $ 50,000.

2004 *Team Lead*, "Provisioning System Design and Team Training", mid-sized ISP, Zurich, Switzerland, $150,000.

2005 *Architecture Lead*, "Provisioning Solution Architecture", large ISP, Germany

2004 *Task Lead*, "Identity Management and Service Provisioning Solution", large corporate environment, USA

2003 *Contract Developer*, "Microsoft Solution for Windows Based Hosting including Hosted Exchange", Microsoft Corporation

2002 *Contract Developer*, "Microsoft Solution for Windows Based Hosting", Microsoft Corporation

2001 *Contract Developer*, "Microsoft Provisioning System, Web Management Console", Microsoft Corporation

2001 *Task Lead*, "Custom Provisioning Solution", large Telco, Tokyo, Japan

2000 *Task Lead*, "Million Mailbox March" (scaling hosted mail platform to support > 1 million subscribers), large software vendor.

Publications

Conference Papers (8)

2020 S. Oesch and **R. E. Gillen** and T. Karnowski. An Integrated Platform for Collaborative Data Analytics. In *13th IEEE International Conference on Cyber, Physical and Social Computing (CPSCom 2020)*, November 2020

2020 **R. E. Gillen** and J. Carter and C. Craig and J. Johnson and S. L. Scott. Assessing Anomaly-Based Intrusion Detection Configurations for Industrial Control Systems. In *2020 International Symposium on a World of Wireless, Mobile and Multi-media Networks: Workshop on Communication, Computing, and Networking in CyberPhysical Systems (WoWMoM-CCNCPS'2020)*, August 2020

2020 **R. E. Gillen** and L. A. Anderson and C. Craig and J. Johnson and R. Anderson and A. Craig and A. Columbia and S. L. Scott. Design and Implementation of Full-Scale Industrial Control System Test Bed for Assessing Cyber-Security Defenses. In *2020 International Symposium on a World of Wireless, Mobile and Multi-media Networks: Workshop on Communication, Computing, and Networking in CyberPhysical Systems (WoWMoM-CCNCPS'2020)*, August 2020

2020 **R. E. Gillen** and S. L. Scott. Massively scalable near duplicate detection in streams of documents using MDSH. In *3RD IEEE International Conference on Industrial Cyber-Physical Systems (ICPS 2020)*, June 2020

2013 P. Logasa Bogen and C. T. Symons and A. McKenzie and R. M. Patton and **R. E. Gillen**. Massively scalable near duplicate detection in streams of documents using MDSH. In *Big Data, 2013 IEEE International Conference on*, pp. 480–486, October 2013, doi:10.1109/BigData.2013.6691610

2013 A. McKenzie and **R. Gillen** and P. Logasa Bogen. Redeye Text Analysis Workbench: Actionable intelligence from non-actionable data. In *Technologies for Homeland Security (HST), 2013 IEEE International Conference on*, pp. 381-385, November 2013, doi:10.1109/THS.2013.6699034

2013 Bogen, Paul L. and McKenzie, Amber and **Gillen, Rob**. Redeye: A Digital Library for Forensic Document Triage. In *Proceedings of the 13th ACM/IEEE-CS Joint Conference on Digital Libraries (JCDL '13)*, pp. 181–190, July 2013, doi:10.1145/2467696.2467716

2013 Beaver, Justin M. and Symons, Christopher T. and **Gillen, Robert E.** A Learning System for Discriminating Variants of Malicious Network Traffic. In *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW '13)*, pp. 23:1–23:4, January 2013, doi:10.1145/2459976.2460003

Patents (2)

2016 Christopher T. Symons, Justin M. Beaver, **Rob Gillen**, Thomas E. Potok. In-situ trainable intrusion detection system. Patent No. US 9497204 B2, issued 15 Nov. 2016.

2014 **Robert E. Gillen**, Robert M. Patton, Thomas E. Potok, Carlos C. Rojas. Cloud computing method for dynamically scaling a process across physical machine boundaries. Patent No. US 8825710 B2, issued 2 Sep. 2014.

Invited Articles (2)

2011 **Rob Gillen**. Digital Forensics and the Cloud. In *FedScoop*, January 17, 2011, https://www.fedscoop.com/digital-forensics-and-the-cloud/

2010 **Rob Gillen**. Cloud Computing: Beyond the Buzz. In *FedScoop*, November 18, 2010, https://www.fedscoop.com/cloud-computing-beyond-the-buzz/.

Open Source (1)

2018 Oesch, Timothy S and **Gillen, Robert E** and Haas, Nicholas Q and and Karnowski, Thomas P. ShareAnalytics - A Collaborative Data Analytics Platform. https://github.com/ORNL/ShareAnalytics

2018 Haas, Nicholas Q and **Gillen, Robert E** and Karnowski, Thomas P. MCR Container Tools. https://github.com/ORNL/mcr-container-tools

Students & Intern Mentoring

2019 Andrew Craig, Tennessee Technological University, MS Computer Science: Error Estimation of Interpolated Data in the SCADA System for Summit Supercomputer Cooling

2019 Jordan Johnson, Tennessee Technological University, MS Computer Science: Attacking SCADA with an ARP Poisoning Man-in-the-Middle Tool

2019 Adam Columbia, University of Texas, San Antonio, BS Cyber-Security: Full-Scale ICS Testbed for Evaluating Cyber-Security Defenses

2019 Rachel Anderson, Massachusetts Institute of Technology , BS Engineering: Full-Scale ICS Testbed for Evaluating Cyber-Security Defenses

2018 Lauren Good, Tennessee Technological University, MS Computer Science: A Survey and Method of Ranking Machine-Learning Based Network Defenses

2018 Andrew Worley, Tennessee Technological University, BS Computer Science: Measuring and predicting speedup of MPI-Enabled applications

2018 Justin Humphrey, Midway Highschool, Environment for testing and monitoring the behavior of malware

2016-2018 Sean Oesch, University of Tennessee Knoxville, PhD Computer Science: User Interface and Systems development for interaction with remote embedded systems

2013 Zachary Taylor, Bob Jones University, BS Computer Science: Named Entity Recognition (NER) in mixed-language texts

2012-2013 Amber McKenzie, University of South Carolina, Linguistics Program, PhD Computer Science: Natural Language Processing (NLP) and large scale text analytics supporting federal law enforcement

2010 Sethuraman Subbiah, North Carolina State University, MS Computer Science: File System in User Environment (FUSE) layer for Eucalyptus, Azure similar to existing S3 implementation

2010 Jonathan Rann, North Carolina A&T State University, MS Computer Security: Design and Development of tools allowing scientific use of cloud computing

2008-2009 Paul Ralph, Bob Jones University, BS Computer Science: Development of business applications supporting scientific environments

Professional Service

Mentoring

2023 Cybersecurity Career Mentor: EC-Council

Conference Organizer

2015-2020 CodeMash Developer Conference - responsible for all content and speaker selections

Program Committee

2017-2019 IEEE International Conference on Fog and Mobile Edge Computing (FMEC)
2013-2018 ORNL Cyber and Information Security Research Conference (CISRC)
2018 IEEE International Workshop on Mobile Cloud Computing systems, Management, and Security (MCSMS)
2017-2018 IEEE/ACM International Conference on Big Data Computing, Applications and Technologies (BDCAT)
2010-2017 IEEE/ACM International Conference on Utility and Cloud Computing (UCC)
2016-2017 ACM/SIGHPC International Workshop on Data-Intensive Computing in the Clouds (DataCloud)
2015-2016 IEEE International Conference on Big Data and Cloud Computing (BDCloud)
2014 Rapid Response Cyber Forensics Workshop (RRCF)
2011-2012 ACM/IEEE International Conference on Grid Computing (Grid)

Journal Reviewer

2016-2018 Cluster Computing, the Journal of Networks, Software Tools and Applications

Conference Reviewer

2016-2018 ACS/IEEE International Conference on Computer Systems and Applications (AICCSA)
2011-2013 International Conference on Cloud and Green Computing (CGC) (2011-2013)

Artifact Reviewer

2020 USENIX Security '20 Fall Artifacts
2019 USENIX Security '20 Winter Artifacts

Review Panel

2019-2020 ORNL SEED Fund, External Assessor

2017 ORNL Laboratory Directed Research and Development (LDRD), Cybersecurity for Energy Infrastructure

2011 DOE Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR)

Media Coverage

2015 "Episode 332: Rob Gillen on Security for Developers", Technology and Friends, Microsoft's Channel 9, July 2015, https://channel9.msdn.com/Blogs/Technology-and-Friends/tf332

2012 "Rob Gillen Secures WiFi!", RunAsRadio Podcast, October 2012, http://runasradio.com/Shows/Show/285

2011 "Bytes by MSDN: Rob Gillen and Dave Nielsen on Windows Azure Big Compute", Microsoft's Channel 9, August 2011, https://channel9.msdn.com/Blogs/Bytes+by+MSDN/Bytes-by-MSDN-Rob-Gillen-and-Dave-Nielsen-on-Windows-Azure-Big-Compute

2011 "Thought Leaders in the cloud: Talking with Rob Gillen, Oak Ridge National Lab Cloud Computing Researcher", Microsoft Azure blog, June 2011, https://azure.microsoft.com/sv-se/blog/thought-leaders-in-the-cloud-talking-with-rob-gillen-oak-ridge-national-lab-cloud-computing-researcher/

2011 "HPC Clouds Defined in Three Minutes", HPC Wire covered an interview given by Gillen and the discussion of how clouds can impact high performance computing, April 2011, https://www.hpcwire.com/2011/04/29/hpc_clouds_defined_in_three_minutes/

2011 "Supercomputers in the Cloud and Azure Blast", Microsoft User Community YouTube channel, March 2011, https://www.youtube.com/watch?v=vtO7j2a0e-k

2010 "Cloud Cover Episode 9 - Blob API", Research on cloud file transfer work discussed on the Microsoft Azure Cloud Cover Show, Microsoft's Channel 9, April 2010, https://channel9.msdn.com/Shows/Cloud+Cover/Cloud-Cover-Episode-9-Blob-API

Presentations & Demonstrations

Presentations & Invited Talks

September 2020 "Method for Accessing Security Impact of Settings in Anomaly-Based Intrusion Detection for Industrial Control Systems", invited talk for the Computer Science Graduate Student Seminar Series, Tennessee Technological University, Cookeville, TN.

October 2019 "A Survey of a Decade of Research at a National Laboratory", invited talk for the Computer Science Graduate Student Seminar Series, Tennessee Technological University, Cookeville, TN.

June 2011 "Scaling Document Clustering in the Cloud", invited talk at the Microsoft Research Cloud Futures 2011 workshop, Seattle, WA.

November 2010 "IT Matters - Panel on Cloud Computing", invited panelist at NASA Goddard - workshop

on cloud computing, Greenbelt, MD.

April 2010 "Panel on Cloud Applications – New Experiences and Expectations", invited talk at the Microsoft Research Cloud Futures 2010 workshop, Seattle, WA.

April 2010 "Data and the Cloud: A Call for Improved Formats and Consistency in Data Services Supporting Scientific Research', invited talk at the Microsoft Research Cloud Futures 2010 workshop, Seattle, WA.

November 2009 "Azure for Climate Analysis", invited talk at the Microsoft Public Sector/Healthcare and Life Sciences Dinner and Cloud Computing Showcase at their 2009 Professional Developers Conference (PDC) in Los Angeles, CA.

September 2009 "Windows Azure: Lessons from the field", invited talk at the September 2009 meeting of the Huntsville New Technology Users Group (HUNTUG) in Huntsville, AL.

July 2002 "Microsoft Provisioning System", internal workshop for Microsoft Field at the Microsoft Global Briefing, New Orleans, LA.

Workshops

January 2014 "Hiding in Plain Sight", "What's in a Password", "Software Defined Radio for the Pen Tester", and "How Well Do You Know Your Runtime?" Invited talks/developer security workshop, CodeMash 2014 developer conference, Sandusky, OH.

January 2013 "Developer Security", 8-hour invited workshop co-presented with Bill Sempf at the CodeMash 2013 developer conference, Sandusky, OH.

January 2012 "Moving to the Cloud?", 4-hour invited workshop co-presented with Michael Wood at the CodeMash 2013 developer conference, Sandusky, OH.

January 2011 "An Introduction to Azure" and "An Introduction to Amazon Web Services" two invited 4-hour workshops delivered at the CodeMash 2011 developer conference in Sandusky, OH.

November 2005 "3-day Training for Microsoft Provisioning System", Microsoft Corporation, Seattle, WA

September 2002 "3-day workshop on Microsoft Hosting Solutions", Hewlett Packard, Banglore, India

August 2001 "Microsoft Provisioning System", Microsoft Japan, Tokyo, Japan.

Conference Talks

Apr. 2019 "How Anomalous is Anomalous", Presentation to the CodeStock 2019 developer conference, Knoxville, TN.

Aug. 2014 "Intro to Reversing" and "Hiding in Plain Sight", Presentations to the DevLink 2014 developer conference, Chattanooga, TN.

July 2014 "Hiding in Plain Sight" and "What's in a Password" Presentations to the CodeStock 2014 developer conference, Knoxville, TN.

October 2013 "Hiding in Plain Sight" and "Anatomy of a Buffer Overflow Attack", Invited presentations at the East Tennessee CyberSecurity Summit, Knoxville, TN.

August 2012 "Anatomy of a Buffer Overflow Attack", "WiFu - So you think your wireless connection is safe?", presentations to the DevLink 2012 developer conference, Chattanooga, TN.

June 2012 "Anatomy of a Buffer Overflow Attack", "WiFu - So you think your wireless connection is safe?", presentations to the CodeStock 2012 developer conference, Knoxville, TN.

September 2011 "A Comparison of Windows Azure and Amazon Web Services" and "Introduction to GPGPU

Development using CUDA", invited presentations at the DevLink 2011 developer conference in Nashville, TN.

June 2011 "A Comparison of Windows Azure and Amazon Web Services" and "Introduction to GPGPU Development using CUDA", invited presentations at the CodeStock 2011 developer conference in Knoxville, TN.

May 2011 "Hands-On with Amazon Web Services" presentation to the StirTREK 2011 Developer conference in Columbus, OH.

August 2010 "Amazon Web Services for the .NET Developer" presentation to the DevLink 2010 developer conference in Nashville, TN.

June 2010 "Amazon Web Services for the .NET Developer" and "Azure: Lessons From the Field", presentations to the CodeStock 2010 developer conference, Knoxville TN.

January 2010 "Windows Azure: Lessons from the field" presenation to the CodeMash 2010 developer conference in Sandusky, OH.

June 2009 "Deployment and Packaging SharePoint solutions using TFS" presentation to the CodeStock 2009 developer conference in Knoxville, TN.

Community Service

2022-present Treasurer, Bakeroos - provides custom birthday cakes to kids in foster care as well as underprivileged youth, `https://bakeroos.org`

2013-present Co-founder, Compassion Closet - outreach to adoptive and foster families providing quick-turn durable goods and supplies, `https://compassioncloset.com`

2018-present Congregational Pastor, Immanuel Church, Knoxville. `https://iknox.org`

2014-2018 Team Orphans' Virtual Ironman Site: Built and Support site as a fundraiser for special-needs adoptions, `http://teamorphans.com`, `http://virtualiron.teamorphans.com`

2016 Helped Codemash conference host and facilitate a toy "hacking" event wherein the conference attendees spent an evening adapting toys for use by special-needs children. The event supported Katelyn's Closet and resulted in 68 toys ready for distribution, `http://www.katelynskrusade.org/katelyns-kloset-2/`

2013 Organized and hosted a metric-century bike ride raising funds to support a family in their special-needs adoption, `http://www.idoitfor.org/connie`

2011-2013 Foster family providing a home for at-risk children