Curriculum Vitae

Terry R. Merz DCS, CISSP, CISM
PACIFIC NORTHWEST NATIONAL LABORATORY
Terry.merz@pnnl.gov

Present Position

Senior Cyber Research Scientist
Pacific Northwest National Laboratory
Richland, Washington

And

Adjunct Professor
University at Albany, College of Emergency Preparedness, Homeland Security and Cyber Security, Albany New York

Education

2012-2017	Doctor of Computer Science, Concentration: Information Assurance, Colorado Technical University, Colorado Springs, Colorado
2010-2012	Master of Science, Computer Science, Concentration: Information Assurance, Colorado Technical University, Colorado Springs, Colorado
1987-1992	Bachelor of Science, Information Systems, Concentration: Software Development University of Maryland, University College, College Park, Maryland

Certifications

Certified Information Systems Security Professional (CISSP), ISC2,
Certified Information Systems Security Manager (CISM), ISACA

Recent Research Efforts

Sept. 2019 – Present: Senior Cyber Research Scientist and DevSecOps Team Lead for the Systems Security Engineering Team on the Department of Energy's North American Resiliency Model (AI in cyber)

January 2018 - present: Cybersecurity researcher and technical team lead for the security architecture for DoD MOSAICS Joint Demonstration Test involving the development of a self-healing, situationally aware reference architecture for power systems.

January 2018 - present: CRISP researcher: Long term exploratory research leveraging 10 years of data collected from commercial industrial control systems (power systems)

Nov. 2017 - present: PI for exploratory, mixed methods: Domain and context variable modeling relative to asymmetric cyber events involving social engineering.

May 2017 - present: Cybersecurity researcher for DoD ESTCP on behalf of PNNL as a sub to LLNL - Exploratory study (Mixed methods): Develop theoretical model for test plan involving demonstration test of binary analysis tools

May 2017 - Sept. 2017: PI for secondary study - The Human-In-The-Loop on Cyber-Physical Systems

Jan. 2016- August 2017: PI for Behavioral Information Security (INFOSEC): Cybersecurity Trained User and Successful Phishing Attacks (2 Quantitative Studies of Policy Compliance Behaviors)

Jan. 2014 – Jul. 2015: Cyber Lead and PI for J-BASICS Joint Test, incident response tactics, techniques and procedures on DoD critical infrastructure

A quantitative study designed to test the efficacy of Tactics, Techniques and Procedures (TTP) relative to the defense of Industrial Control Systems (ICS) against Nation State level cyber-attacks.

Scholarly Papers

Sept. 2017: The Cybersecurity Trained User and Successful Phishing Attacks
Aug. 2017: The Human-in-the-Loop
Oct. 2017: Behavioral Information Security: Phishing for Answers
Mar. 2018: A National Energy Infrastructure Profile: Baselining the Current State of U.S. Energy Systems
Sep. 2018: The Science of Cyber Operations: Phishing, User Habits and Protection Motivation A Quantitative Study of User Behaviors and Cybersecurity Policy Compliance
June 2019: A Context Centered Research Approach to Phishing and Operational Technology in Industrial Control Systems
April 2019: Mapping Cyber Deception Techniques by Leveraging Contextual Data Models to Profile and Predict Potential Cyber Threats to Industrial Control Systems
May 2020-Present: Co-authoring a book relative to Human Behaviors and Cybersecurity for the British Institution of Engineering and Technology. Expected completion date December 2022

Speaking Engagements

DOE CyberCon	April 2018: Social Engineering and Policy Compliance Behaviors
DOE Cyber Webinar	Oct 2018: Phishing and Context Centered Research
CSIAC	Dec 2018: "Phishing for Solutions": Quantitative, Contextual Research
Los Alamos National Lab	Feb 2019: Research, Social Engineering, and Context Centered Studies
IP3	April 2019: Research, Social Engineering and Context Centered Studies
CEHC, State of Grace	Oct. 2019: "Phishing for Solutions, a Research Journey"

University Teaching Experience

State University of New York at Albany, College of Emergency Preparedness, Homeland Security and Cybersecurity (CEHC): **Dates:** Aug. 2019 – Present

Currently serving as an adjunct professor teaching senior undergraduate students, and graduate students (to include PhD students). Specific accomplishments include:

- Successfully guiding PhD students towards their first publication in fulfillment of their graduation requirements
- Transitioning in-class room curriculum to online curriculum mid-semester
- Converting in-person curriculum to online class and creating a continuous support structure for students unaccustomed to online learning

Course curriculum developed, taught, and currently teaching:

CEHC 310: Research Seminar in Emergency Preparedness Homeland Security and Cybersecurity (3 Credits)

CINF 465: Senior CAPSTON Informatics (3 Credits)

CINF 454/554: Human Aspects of Cybersecurity (3 Credits)

CINF 723: Information and Computing (2 Credits)

Professional Experience

Pacific Northwest National Laboratory (PNNL) **Dates:** May, 2017 - Present
Position: Senior Cyber Research Scientist

Duties and Responsibilities

Conduct primary and secondary research of cybersecurity technologies, tactics, techniques and procedures using quantitative, qualitative, and mixed methods approaches relative to operational technologies (OT), and behavioral information security. Leverage PNNL's computational analytics, High Performance Computing, and software engineering capabilities to form cross disciplinary research teams for Lab Directed Research and Development efforts. Focusing on applied research, develop prototypes for rapid sponsor deployment. Actively pursue publishing opportunities in academic and scientific journals, and support community STEM initiatives. Establish relationships with local universities and explore joint research opportunities in the areas of cybersecurity, operations and behavioral information security. Develop, coordinate and produce a Cyber Incident Response course for Federal Law Enforcement for entry level responders as well as advanced incident responders.

U.S. Army, PEO C3T **Dates:** July 27, 2015 - May 21, 2017
Position: Chief Information Security Officer/Principal Cybersecurity Architect (Civil Service)

Duties and Responsibilities:

Serves as the Chief Information Security Officer within the office of PEO C3T's Cyber Operations & CIO Directorate. Develops, directs and implements an overall cyber strategy to include establishing overarching technical and programmatic plans to achieve cohesive and complete cyber compliance and capability across the Army's tactical communications and command & control programs. Implements Army Cyberspace strategy, policy, programs, operational concepts, and initiatives within the PEO's portfolio of capability.

US CYBERCOM, J5, J-BASICS **Dates:** 02/27/2014- July 27, 2015
Position: Cyber Security Principal Investigator for J-BASICS Joint Test

Duties and Responsibilities:

For the Joint Test, J-BASICS provide Cyber Team Leadership for the development of Tactics, Techniques and Procedures (TTP) relative the protection of Supervisor Control and Data Acquisition (SCADA)/Industrial Control Systems (ICS) from Nation State level attacks.

Duties include: Analyzing and reverse engineering Advanced Persistent Threats (APT's) in a laboratory environment. Capture and characterize APT symptoms and develop Tactics, Techniques and Procedures (TTP) responses that detect, mitigate and recovery from an ATP (APT types include user, operating system and firmware level rootkits). Map APT attack paths, and conduct research on additional threats vectors. Develop table top Red Team exercises against the TTP, and provide analysis of SANDIA Red Team MSELs designed to be used to test TTP . Provide user participants training on the use of SNORT, Kali, Security Onion, SysInternals, Kabana, and Netflows. Develop white papers for the customer

around resultant test issues and additional research opportunities. Provide Cyber Team with TTP development framework, manage development schedule, quality control, review and delivery.

Cynergy Group of Baltimore, Inc. **Dates:** 01/04/2002 – 02/27/2014

Position: Owner/Principal Cyber Security Engineer

Duties and Responsibilities: Develop Cynergy's cyber security engineering service offering, manage Cynergy's operations, and provide cyber security engineering services to the following Cynergy customers:

Client: SafeNet, Assured Decisions LLC **Dates:** 11/2012 - 03/2013
Position: Principal Information Systems Security Engineer

Duties and Responsibilities:

Provide security engineering support to the SafeNet AD Network Architect in the role of Senior ISSE. As the Senior ISSE, evaluate government client's threat profiles (USMC) and develop attack vectors for the development of rule sets designed to be implemented into the analytical tool set entitled Situational Awareness and Risk Assessment (SARA). Evaluate audit data from Marine perimeter devices (McAfee ESM, and ePO –HBSS-, vulnerability scanners, identity authentication management systems, perimeter firewalls), develop event context (user, application behaviors), and create event schemas for the development of SARA rule sets.

Client: US Marine Corps MCWEST **Dates:** 05/2012 to 11/2012
Position: Information Systems Security Engineer SME for Special Projects

Duties and Responsibilities:

Provide direct support and direction to contractor team serving the Regional Information Assurance Manager. Provide SEIM solutions development for the MCWEST Computer Network Defense program. Evaluate various security architectures featuring real time cyber "Situational Awareness" for efficacy. Evaluate collection and analytical rates of SEIM solutions, and HBSS, develop recommendations and white papers for the Regional CIO (G6). Evaluate the implementation of the Application Identity and Access Management (IdAM) and its impact on regional system performance. Assist the regional IAM in developing role based schema for the implementation of discretionary access controls using IdAM for Regional Applications.

Client: Director of National Intelligence **Dates:** 11/2011 to 05/2012
Position: Principal Information Systems Security Engineer

Duties and Responsibilities:

Provide independent security engineering support to the Director of National Intelligence Certification and Accreditation Test Team (CAT Team). Support included system engineering support in response to CAT team audits. Assisted clients in the development of ICD 503 compliant packages, preparing test plans, conducting security testing using DNI approved testing tools, such as Backtrack, and WebInspect. Developed strategies and recommendations for systems migrating from DCID 6/3 to ICD 503 processes. Developed senior level reports for the DNI customer for submission to the IC CIO.

Client: Commander Navy Installations Command (CNIC**)** **Dates:** 01/2009 – 11/2011

Position: Cyber Team Lead for CNIC Contractor Team

Duties and Responsibilities:

Enclaves, Systems, Major Applications: Serve as a Fully Qualified Navy Validator for the Commander Navy Installations Command as well as Information Systems Security Officer for CNIC Systems Operation Center, and the Cyber Team Lead for the Incident Response Team as well as the Certification and Accreditation Team. Evaluate SOC system security posture on a wide variety of systems to include enclaves, networks, hosts and virtual environments. Provide threat analysis and statements of residual risk to the Certification Authority and the Operational Designated Approving Authority.
Provide technical team leadership and security engineering services to multi-contractor team for blue team vulnerability assessments worldwide. Use tools such as Eye Retina, DISA Gold Disk, NSA SNAC guides, Backtrack v. 5, nmap, Nessus and various other tools (for example wireless assessments (Commview)) in executing validation visits on systems world wide.
Collect forensic data and conduct analysis on samples taken from sites using Government Off the Shelf (GOTS) tools. Review security architectures and provide guidance to Navy sites re: compliance with DISA STIGs, and NTD 0808. Validate Certification and Accreditation packages, conduct Risk Assessments and develop Certification Determinations for submission to the Designated Approving Authority.

SCADA Systems
Integrate with the SCADA development and implementation team to ensure Department of Defense (DOD), Department of the Navy (DON) and the North American Electrical Reliability Corporation Critical Infrastructure Protection (NERC-CIP) security standards are adhered to. Provide security engineering guidance to SCADA stakeholders relative to the development of secure interfaces between disparate systems (for example legacy, and wireless metering systems). Conduct security vulnerability assessments against CNIC SCADA and AMI using vulnerability scanning tools such as Nessus (with Bandolier audit file plugins). Provide remediation and security design recommendations for SCADA systems. Evaluate Smart-Grid implementations for vulnerabilities and identify mitigation strategies as needed.

PCI DSS
Conducted security audits against point of sale systems as well as retail systems processing credit cards for DoD retailers. Evaluated systems against PCI DSS requirements, provided recommendations and directed mitigation strategies.

Client: National Security Agency **(NSA)** **Dates:** 01/2009 – 11/2016
Position: Lead instructor

Develop curriculum and provide adult educational instruction to NSA employees in the areas of systems engineering and systems security engineering.

Additional Clients supported while at Cynergy Group of Baltimore, Inc.

Client: Florida Department of Law Enforcement
Dates: March 2008 – January 2009
Position: Senior Information Systems Security Engineer

Integrate with development team of statewide law enforcement system and provide systems security engineering life cycle support: develop security requirements in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-53, provide security architecture, and design.

Conduct risk assessment against proposed product list. Develop security integration tests, focusing on Community of Interest (COI) interfaces. Develop Systems Security Plan**.**

Client: US Navy, SPAWAR, Deployable Joint Command and Control System (DJC2)
Dates: January 2004- March 2008
Position: Cybersecurity Interim Program Team Lead (IPT)

Cybersecurity IPT lead and Senior Security Engineer for the Space and Naval Warfare (SPAWAR) effort involving the Deployable Joint Command and Control (DJC2): provided security requirements definition and evaluation of legacy systems for integration into the DJC2 baseline, provide review and analysis of security architecture, provide vulnerability assessment of product lists, review Systems Security Authorization Agreements (SSAA) and provide guidance and correction as needed prior to delivery to NETWARCOM

Client: Federal Bureau of Investigation (FBI)
Dates: January 2003 – January 2004
Position: Certification Team Lead/Senior Information Security Engineer

Certification Team Lead and Senior Information Security Engineer: provide Certification and Accreditation support to the Certification Unit of the FBI. Conduct vulnerability assessments against a wide variety of architectures, to include classified and unclassified systems. Provide security-engineering support and leadership by evaluating security requirements against NIST, DCID 6/3 and FBI standards and guidelines, provide architecture and design recommendations. Develop threat analysis briefings for senior FBI personnel, and statements of residual risk.

Additional Employers (Additional Details can be provided if needed)

Employer: Veridian Corporation, Falls Church, VA
Dates: August 2000- January 2003
Position: Technical Task Leader/Senior Information Security Engineer

Clients: U.S. Central Command, Deployable Headquarters
Global Command and Control System – Joint (GCCS-J)
Cybersecurity Interim Program Team Lead

Employer: Booz-Allen and Hamilton, Fairview Park VA
Dates: March 1998 to August 2000
Position: Information Assurance Task Lead/Senior Information Systems Security Engineer

Clients: General Services Administration (GSA)
U.S. Navy, SPAWAR
Information Assurance Task Lead

Employer: Fannie Mae, Washington, DC
Dates: March 1998 to July 2000
Position: Technical Risk Specialist

Employer: Naval Security Group Activity Pensacola, FL.
Dates: March 1996 to February 1998
Position: Lead Programmer (ADA and ANSI C) Tactical Intelligence Network (TACINTEL) Team Lead (Civil Service)

Employer: Department of Education, Child Development Services, Augusta ME
Dates: 1993 to 1996
Position: Programmer, and WAN/LAN Project Coordinator/Information System Security Engineer

Employment: Higgins Office Products
Dates: 1991 – 1993
Position: Software Engineer

Employment: Active Duty, U.S. Navy, Position: ISSO and ISSM, Dates: 1984- 1991