Last Updated January 12, 2024

Software Engineering and Cybersecurity Laboratory (SECL)

https://www.montana.edu/cyber/

We are an interdisciplinary team of computer and data scientists and software engineers who take aim at vexing problems using convergent scientific and engineering approaches.

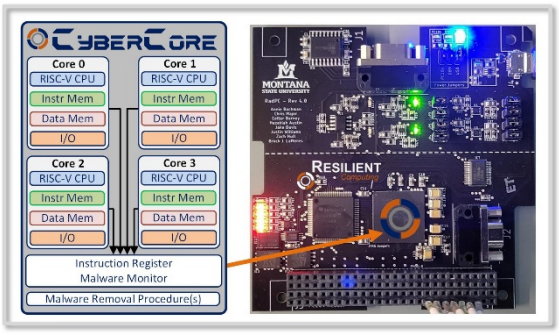
Co-Directors: Drs. Clem Izurieta and Ann Marie Reinhold
Faculty: Drs. Brock LaMeres, Bradley Whitaker, Matthew Revelle, Fangtian Zhong, and Derek Reimanis
Program Manager: Ms. Suzie Hockel
Students: 10 PhD students, 3 MS students, 6 undergraduate researchers

Funding: NSF, DoD (Griffiss Institute), DHS, INL, CERL, Army, Air Force, Raytheon, NASA, TechLink, Blackthorne, and other private industry.

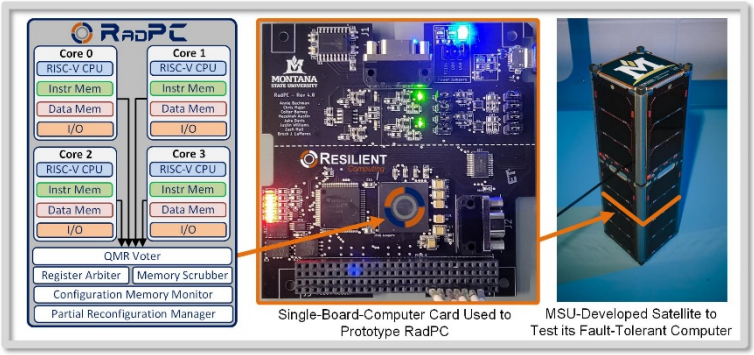
SECL Cybersecurity Current Projects: Our cyber research employs a unique approach to protecting IT and OT systems by providing a Quality Assurance (QA) perspective to identifying weaknesses and vulnerabilities in systems.

1) Hierarchical Software Quality Assurance (HSQA) protects systems along the supply, build, and development paths by allowing cyber professionals to deploy quality gates to filter potential threats. HSQA models provide layered and holistic overviews of assets. This novel technology leverages existing static analysis methods as inputs and scores the quality and security of software artifacts. Scores are provided at multiple levels in the hierarchy—with audiences that range from developers to project managers to C-suite executives. Existing models measure the quality and security of binaries, C, and C# source code. Model development is underway to measure source code quality and maturity of Industrial Control Systems (ICS), software and hardware bills of materials (SBOMs and HBOMs), and Azure cloud environments. Future work involves the identification of security zones and sensitive sections of source code and the development of models to secure EV infrastructure in collaboration with the Pacific Northwest National Laboratories (PNNL).

2) We employ hardware diversity to impart resistance to malware. We are developing a novel computing approach called CyberCore (Computer Obfuscation for Reliable Execution) that can detect and defeat malware using hardware diversity in edge computers. CyberCore implements functionally equivalent, redundant, heterogeneous, computer cores on a Field Programmable Gate Array (FPGA) and secures the outputs via a voting system. In the event of a malware attack, CyberCore will detect the malware as unknown instruction codes and flag the event. Once the computer detects an attack, the FPGA moves into a safe mode to continue processing. This research aims to provide an additional level of malware protection for critical computing applications.



3) We are developing a novel fault tolerant flight computer for use small spacecraft that must operate in harsh radiation environments. The approach called *RadPC* implements redundant computing cores on an FPGA, each can be partially reconfigured to its initial state independent of each other. This allows the system to produce a system output based on the majority of results from the cores in the event one core is faulted. In the event of a fault, the effected core is partially reconfigured to flush out any radiation-induced faults and then reintroduced into the system. RadPC has been flight tested on balloons (9x), sounding rockets (2x), the International Space Station (3x), and small satellites (2x). In 2023, it traveled to the surface of the moon for its harshest test yet.



4) We are developing pipelines to assess the accuracy and trustworthiness of cybersecurity static analysis tools and aggregate their findings. Static analysis tools aim to investigate the security of software artifacts; our team is documenting variation in tools attributed to tool version, vendor, configuration settings, and environments. This research provides essential information to inform the selection of tools and to form a baseline against which comparisons across software artifacts and tools can be made.

5) We are using data science approaches to identify co-occurrences of cyber threats. We are developing pipelines to identify and group "families" of software artifacts having shared weaknesses and vulnerabilities. Here, we employ dimensionality reduction techniques and hierarchical clustering to group suites of software artifacts based on the weaknesses identified via open-source tools (e.g., CWE Checker, Yara Rules, CVE Bin Tool). Pipelines are extensible to closed-source tools as well.

6) We are developing a tool to enable detection of security vulnerabilities during the development phase of a project. Our novel software takes reports generated by a commonly used static analysis tool, SonarQube, and automatically converts them into GitLab issues. This tool leverages both the API's of SonarQube and GitLab to retrieve and post issue data. The need for such a tool arose from a case when SonarQube's reports were behind a firewall, and only a few developers had access to them. The tool addresses this problem by placing outputs in a place that is familiar to developers: the issues section of a GitLab repository.

7) We are developing machine learning algorithms to enable decode of full-duplex network signals as they appear when passively observed. This applied cyber-physical research will leverage advances in artificial intelligence to countervail physical phenomena resulting from the superposition of electromagnetic waves. Success will allow passive capture and decode of data from Gigabit Ethernet and related communication protocols without prior knowledge of what either endpoint has transmitted. The resulting new technology will enable a completely passive device to interface with and collect data from all communications networks without risk to critical systems resulting from disturbance or delay of signals.

8) We are developing data visualization-assisted techniques aimed at addressing challenges in malware analysis and vulnerability analysis across various architectures, compilers, and

optimizations. Our approach emphasizes robust theoretical guarantees and high-performance outcomes. To achieve our objectives, we utilize binary analysis and context-sensitive feature engineering to capture the crucial semantics of program execution and subsequently quantify these semantics through data visualization. Our methodology involves the formalization of hidden structures within the data, followed by the design of efficient algorithms. These algorithms leverage techniques such as non-convex optimization and tensor decomposition to effectively group the artifacts of programs.

SECL Interdisciplinary Projects: The SECL team prides itself on applying data science and software engineering to solve highly interdisciplinary, wicked problems across scientific domains from computer science to social science to environmental science.

1) We are employing computationally enhanced risk communication to bolster hazard preparedness across domains from cybersecurity to natural hazards. Our team's research in risk communication surmounts the enduring problem of poor message efficacy due to imprecise and ad hoc message construction and is applicable across risk and hazard domains. The efficacy of this approach has been validated and verified experimentally, but the implications of this research extend well beyond academia. We are working towards enhancing the efficacy of risk communication in various real-world applications, providing valuable contributions to fields like public health, crisis management, and cybersecurity readiness. Current work embeds artificial intellegence within our Domain Agnostic Risk Communication (DARC) Framework to improve the efficiency associated with message creation and the efficacy of resultant messages. In an ongoing pilot study in collaboration with VMASC, our team will soon be testing messages built with this framework across the following hazard types: cyber phishing, active shooter, insider threats, and natural hazards.

2) We are using best practices in software engineering in the development of reactive transport models. Clean water is a keystone of resilient coupled natural-human systems. Modeling how solutes (e.g., nutrients, contaminants) are transported and processed in ground and surface waters is a critical scientific objective. Water transport is a primary control on water quality as solutes are transported and thereby redistributed by water. Across spatial scales from soil columns to catchments, water moves via a suite of flowpaths with varying residence times; some water moves "fast" and other water moves "slow." The solutes provided to these waters and the accumulation of residence times governs safety and quality of the water. Our team is merging the fields of earth science and software engineering to create parsimonious reactive transport modeling software. Our work is enhancing the earth scientist user experience and improving environmental monitoring and prediction.

New faculty and staff in our laboratory have improved our capability to perform ML/AI, vulnerability research, reverse engineering, program analysis, and computer network operations (CNO).

SECL Cybersecurity Former Projects: We have expertise in areas from prior work:

1) We can perform cluster-based analysis of malware to detect malware before it causes damage and to better understand "families" of malware. This research uses graph-based machine learning methods; we explore a cadre of graph representations of binary files, such as control flow graphs and function call graphs. We convert these graphs to vectors using graph embedding algorithms and create machine learning models to detect or cluster malicious binaries. Our goal is to explore the effectiveness of different graph representations to discover which ones provide accurate results for detecting and clustering malware.

2) We can improve the confidence of artificial intelligence through improved software testing approaches. We employ Software Engineering for Machine Learning (SE4ML) to improve development, testing, operation, and maintenance of ML models. The focus of this research is on the testing aspect of ML applications by adapting the traditional software testing approaches for improving the confidence in them. Specifically, we employ statistical metamorphic testing techniques to evaluate NN-based classifiers; and explore generic metamorphic relations to test unsupervised algorithms from both the verification and validation perspective.

Commercialization of SECL Technologies:

The CyberCore and RadPC technologies have been licensed to the MSU spin-out company *Resilient Computing*. Through SBIR and seed funding, MSU and Resilient Computing are working toward product development for commercial versions of the MSU technologies. The RadPC technology has been jointly patented with MSU and Resilient Computing and CyberCore is *patent pending*.

Sponsored Research Support:

The HSQA project addresses three areas that align with DHS S&T long term strategies:

1. Measure source code quality and maturity of ICS and cloud based software
2. Composition, stylometry and origination of software
3. Identify secured and sensitive sections of source code

Construction Engineer Research Lab (CERL)
We work with the TSEAL team at TechLink to test software components as well as provide support for measuring the quality assurance of these software components.

NASA
NASA is working with SECL to investigate intrusion-tolerant space computing technologies.

Resilient Computing
We collaborate with this MSU-spin out on the commercialization of edge computing technologies that are used in space and in our nation's critical infrastructure.

Hoplite Industries
We collaborate with MSU's Software Engineering and Cybersecurity Laboratory by providing access to resources, training and providing internships to ROTC cadets

through our CySER grant in collaboration with Griffiss Institute and Washington State University. Hoplite is also engaged in helping us verify hardware components.

WolfSSL
We are working with MSU to help test the neXtECU controllers to increase cybersecurity protection.

Department of Homeland Security/Idaho National Labs
We have developed a framework that allows managers to make informed decisions and gives developers more visibility into code vulnerabilities.

Research Experiences for Undergraduates (REU) and NSF Signals in the Soil (SitS)
The REU summer program provides an opportunity for students from around the country to come to MSU for an immersive summer learning experience. The SECL is leading the software development, validation, and verification for the MSU NSF SitS team.

Raytheon
Building on MSU's prior research on building fault-tolerant computers for NASA, we design hardware diversity to make flight computers resilient to cyber-attacks.

Northwest Virtual Institute for Cybersecurity Education and Research (CySER)
As part of this inter-institution program, ROTC cadets at MSU participate in a baseline cybersecurity class their first semester and carry out a senior capstone project.

Blackthorne
Blackthorne Consulting is working with SECL to investigate new digital forensics techniques.

Contact Information:

Dr. Clemente (Clem) Izurieta
Professor of Computer Science
Co-Director Software Engineering & Cyber Security Lab (SECL)
Idaho National Laboratories Joint Appointment
Pacific Northwest National Laboratories Joint Appointment
Gianforte School of Computing
Montana State University
Office: (406) 994-3720
clemente.izurieta@montana.edu
http://www.gsoc.montana.edu/izurieta

Dr. Ann Marie Reinhold
Assistant Professor
Co-Director Software Engineering & Cyber Security Lab (SECL)
Gianforte School of Computing
Montana State University
Office: (406) 994-5093
annmarie.reinhold@montana.edu
https://www.amreinhold.com
https://www.montana.edu/cyber