CySER Cybersecurity Efforts at Montana State University

November 8, 2022
Dr. Clemente Izurieta
Professor of Computer Science
Software Engineering Laboratory (SEL)
Montana State University

unclassified
Bozeman: Pop ~50,000
Widely accessible outdoor recreation
Significant industry presence
Classified Research

~17,000 students
~93% U.S. Citizens
R1 Carnegie -Very High Research Activity
18:1 Student/Faculty Ratio

8 Ph.D.
4 MSc
1 PostDoc
3 undergraduates
# Software Engineering Laboratory Current Funding

**Students:** 8 Ph.D., 4 MS, 4 Undergraduates, 1 Postdoc

<table>
<thead>
<tr>
<th>Organization</th>
<th>Amount</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Science Foundation</td>
<td>$400K</td>
<td>‘20–’23</td>
</tr>
<tr>
<td><strong>Washington State University/Griffiss Institute</strong></td>
<td>$162K</td>
<td>‘21–’22</td>
</tr>
<tr>
<td>Air Force, Army, CERL</td>
<td>$1.2M</td>
<td>’16 – ongoing</td>
</tr>
<tr>
<td>Raytheon Technologies</td>
<td>$330K</td>
<td>‘21 – ongoing</td>
</tr>
<tr>
<td>Idaho National Laboratory and Department of Homeland Security</td>
<td>$3.1M</td>
<td>‘20 – ’22</td>
</tr>
<tr>
<td>Resilient Computing</td>
<td>$150K</td>
<td>‘22 – ongoing</td>
</tr>
</tbody>
</table>

*Resilient Computing*
Research Collaborations

Hoplite is a leading-edge cybersecurity company specializing in the mitigation of cyber risks. Founded in 2013, Hoplite Industries has developed a set of automated cyber defense capabilities and specialized AI solutions driven by cyber research at a global scale.

Cybercore brings together experts in critical infrastructure security assessments, cyber forensic analysis, threat detection and consequence-based targeting to provide real-world technical solutions and innovations that protect operational environments from an ever-evolving threat landscape.
Army ROTC Bobcat Battalion
CySER/VICEROY

CySER VICEROY to Date

- Identified 2x AY23 Participants
  - 1x Conservation Biology & Ecology
  - 1x Environmental Science & Astrobiology
- All Participants’ Graduation Capstone Projects include Cyber Security Components
- 10 Meetings w/ Grad Advisor/Mentor Complete + Seminars
- Coordinating Internship/EAD De-Conflicts in Summer 2023

Student/Cadet Demographics: 107 Total

- MSL5/Completion: 9
- MSL401 (Senior Year): 14
- MSL301 (Junior Year): 25
- MSL201 (Sophomore Year): 26
- MSL101 (Freshmen Year): 33

Academic Majors: 107 Total

- Tech/TEM
- Non-Tech/STEM

Prior/Projected Commissioning/Career Production

- AY 2016: 10
- AY 2017: 10
- AY 2018: 10
- AY 2019: 10
- AY 2020: 10
- AY 2021: 25
- AY 2022: 15
- AY 2023: 10
- AY 2024: 10
- AY 2025: 10
- AY 2026: 10
AFROTC Detachment 450
CySER/VICEROY

CySER VICEROY to Date
- Identified 2x AY23 Participants
  - 2x Mechanical Engineering
- All Participants’ Graduation Capstone Projects include Cyber Security Components
- 10 Meetings w/Grad Advisor/Mentor Complete + Seminars
- Coordinating Internship/EAD De-Conflicts in Summer 2023

Student/Cadet Demographics: 80 total
- AS700/800 (Complete): 13
- AS300 (Junior Year): 11
- AS400 (Senior Year): 8
- AS200 (Sophomore Year): 19
- AS100 (Freshman Year): 29

Academic Major: 80 Total
- Tech/STEM 52%
- Non-Tec/STEM 48%

Prior/Projected Commissioning/Career Production

2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
- Book Club
- Introductory course in cybersecurity (University of Idaho)
- Independent study credit
- HackerCats club
Education

• Associates degree in Cybersecurity (Gallatin College)
• MS in Cybersecurity
  • Board of Regents approved
  • Seeking CAE certification
• NSF REU program – Cybersecurity algorithms
• Griffiss/DoD program to train 4 ROTC cadets on a yearly basis before commissioning
CySER Participants:

**Institutional PI:** Dr. Clemente Izurieta  
**ROTC Air Force:** Lieutenant Colonel Lance J. Ratterman  
**ROTC Army:** Lieutenant Colonel Christopher L’Heureux  
**Graduate Research Assistant:** Andrew Fallin  

2021-2022 Academic year: 4 Air Force cadets  
2022-2023 Academic year: 2 Air Force and 2 Army cadets
Hierarchical Software QA Modeling

Standards
- ISO/IEC 9126:2001
- ISO/IEC 25010:2011
- NIST 800-53/82
- RMF (Risk Management Framework)

Quamoco (2012 Wagner et al.)
Qatch (2017 Miltiades et al.)
PIQUE (2020 SEL MSU)
CWE-699 View Structure

Microsoft STRIDE

<table>
<thead>
<tr>
<th>Threat</th>
<th>Property Violated</th>
<th>Threat Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>Spoofing identity</td>
<td>Authentication</td>
</tr>
<tr>
<td>T</td>
<td>Tampering with data</td>
<td>Integrity</td>
</tr>
<tr>
<td>R</td>
<td>Repudiation</td>
<td>Non-repudiation</td>
</tr>
<tr>
<td>I</td>
<td>Information disclosure</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>D</td>
<td>Denial of service</td>
<td>Availability</td>
</tr>
<tr>
<td>E</td>
<td>Elevation of privilege</td>
<td>Authorization</td>
</tr>
</tbody>
</table>

Diagram showing relationships between threats and security categories.
PIQUE Models

- Pique-Bin (INL, DHS)
- Pique-C# (CERL Army, Air Force)
- Pique-C#-Sec (CERL Army, Air Force, DHS)
- Pique-Azure (DHS)
- Pique-C++ (DHS)
- Pique-Cloud (DHS)
- Pique-ICS (DHS)
Classification, clustering, and anomaly detection using graph representations of code

Graph data: graph representations (e.g., control flow graphs) of benign and possibly malicious binaries

Extract graph representation using disassembler such as angr

Extract vector representation using graph embedding method such as Graph2Vec

t-SNE visualization of the DBSCAN clustering of the Graph2Vec embedding of the DBC dataset (64 embedding dimensions)
Decomposition of CWE-200

Identify security zones and sensitive sections of source code
Assess the composition, stylometry and origination of software to verify that they are truthful, complete and accurate
Improving the confidence of machine learning models through improved software testing approaches

Intrusion Detection Systems
Conceptual Frameworks and Theory of Bug Bounty Platforms
Malware detection using obfuscation of Opcodes in FPGAs
Current ROTC Students

Zebedee Kumley (AF): Mechanical Engineering
Caleb Lowe (AF): Mechanical Engineering
Tyler Moravec (AR): Conservation Biology and Ecology
Macy Schowalter (AR): Environmental Science and Astrobiology
The students are doing a survey of cybersecurity’s role in modern warfare. They will research the current and future uses of cyber warfare and cyber defense. They will then synthesize this information into a database using the software Neo4j, allowing the students to have a visual, interactive database. They will further develop various campaign “case studies” using INL’s Structured Intelligence Threat Modeling (STIG) software. This software will allow students to analyze the data that they have gathered in a modeled military campaign and see how cyber threats interact on the battlefield.
The students will purchase and test a laser for their capstone project. As part of this project, they will identify potential vulnerabilities in the laser’s digital controls and how best to counteract them. For example, requiring user authentication before the laser can be used. Potential vulnerabilities that will be researched include whether the laser once hooked up to the internet, could be affected by bad actors. Can they increase or decrease the power output, and who is be able to gain access to the physical device. Depending on the identified vulnerabilities, the students will implement some simple counter measures to protect the laser.
MSU’s Applied Research Laboratory

Expanding MSU’s ability to partner with industry and government to provide students with opportunities in classified research.
ARL FEATURES

Secure Research Facility

- 8 DOD accredited laboratory spaces (closed areas) at 1,000 square feet each
- 5 laboratory spaces built to ICD-705 (SCIF) standards - various sizes available
- Cutting edge security system
- Natural gas, clean compressed air, heating & cooling water
- Secret Internet Protocol Router (SIPR) Network access in progress
- Private loading bay with building access
- State of the art conference room
- Backup generator
- Access to MSU Engineering and Science undergraduate and graduate students
- DoE accreditation in progress
MSU’S “Big 8” RESEARCH CAPABILITIES

- Optics and Photonics
- Quantum Advanced Applied Materials
- System Engineering & Prototyping
- Information Assurance
- Cube-Satellite Platforms
- Cybersecurity
- Materials engineering and Characterization
- Experimental Mechanics and Diagnostics
MSU Research Expertise

- Reconfigurable computing, embedded systems, optics, lasers, MEMS/MOEMS, acoustics and audio, communications, power electronics
- Software engineering, software evolution, robotics, computer vision, computational geometry, scientific computing, parallel computing, artificial intelligence, machine learning, data mining, large-scale data analysis
- Design and manufacturing, systems engineering, measurement systems and experimental mechanics, composite structures
- Coherent Lidar/LADAR, Digital Holographic Imaging, Quantum Information Processing, Spatial-Spectral Holographic Microwave Photonics,
- Small satellite programs with executed flight hardware
- Materials Science and Engineering, Optical and Quantum systems, condensed matter