CySER Cybersecurity Efforts at Montana State University

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

- 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

National Science Foundation	$400K (‘20-’23)
Washington State University/Griffiss Institute	$162K (‘21-’22)
Air Force, Army, CERL	$1.2M (’16 – ongoing)
Raytheon Technologies	$330K (‘21 – ongoing)
Idaho National Laboratory and Department of Homeland Security	$3.1M (‘20 – ’22)
Department of Homeland Security	$4.47M (‘22 – ’25)
Resilient Computing	$150K (‘22 – ongoing)

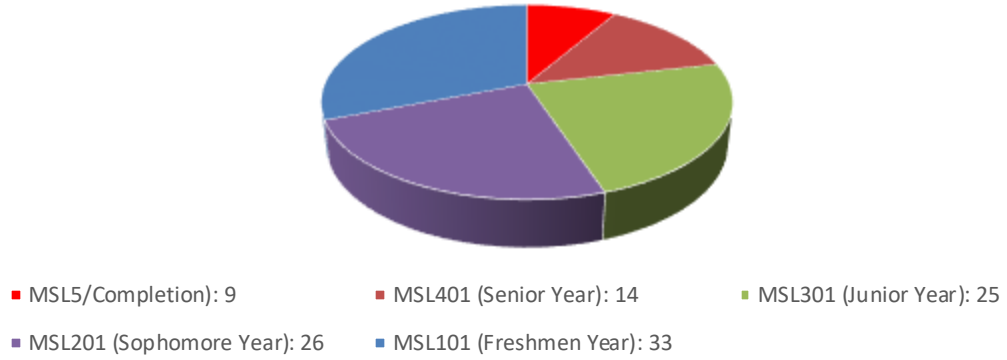
Research Collaborations

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

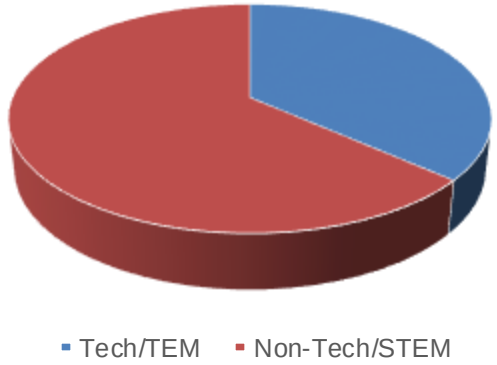
Cybercore brings together experts in critical infrastructure security assessments, cyber forensic analysis, threat detection and consequence-based targeting to provide real-world technical solutions and innovations that protect operational environments from an ever-evolving threat landscape.

Army ROTC Bobcat Battalion
CySER/VICEROY

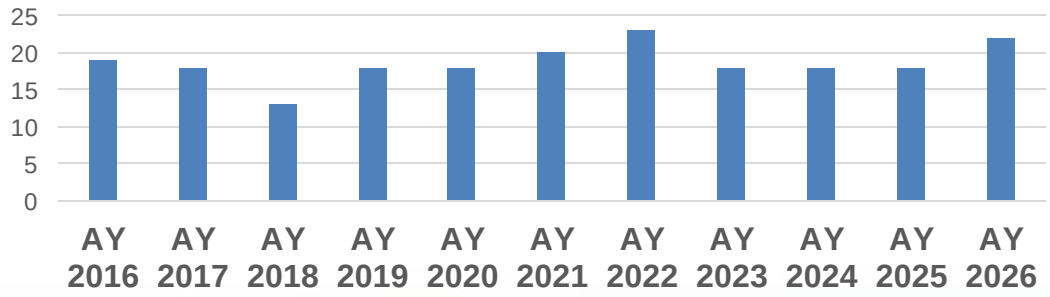
Student/Cadet Demographics: 107 Total



Academic Majors: 107 Total



Prior/Projected Commissioning/Career Production

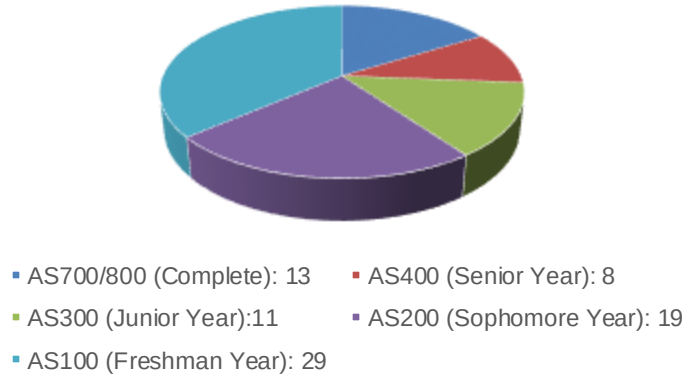


CySER VICEROY to Date

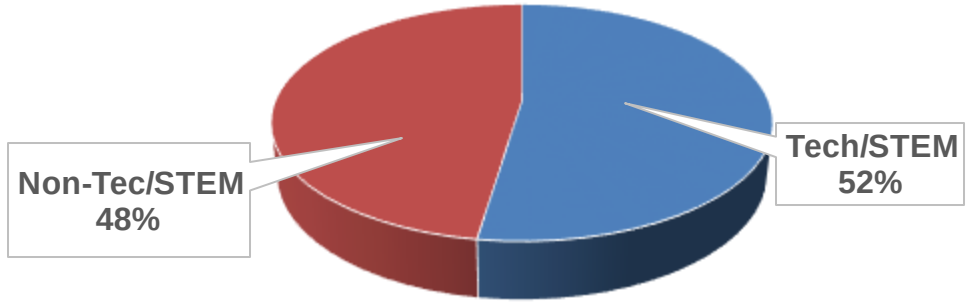
- **Identified 2x AY23 Participants**
  - **1x Conservation Biology & Ecology**
  - **1x Environmental Science & Astrobiology**
- **All Participants' Graduation Capstone Projects include Cyber Security Components**
- **10 Meetings w/Grad Advisor/Mentor Complete + Seminars**
- **Coordinating Internship/EAD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

AFROTC Detachment 450
CySER/VICEROY

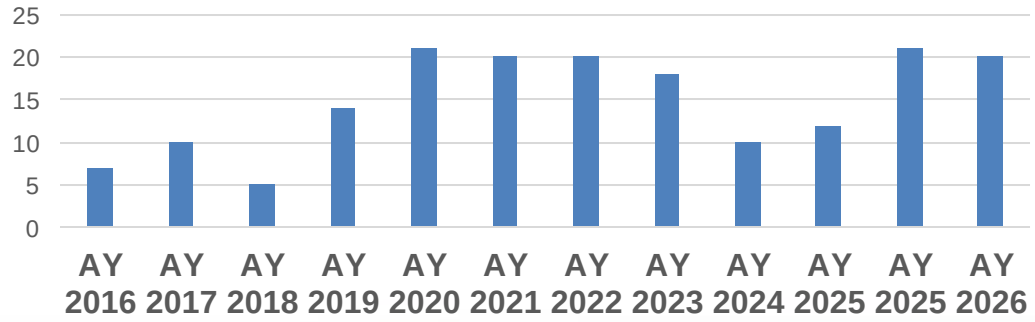
Student/Cadet Demographics: 80 total



Academic Major: 80 Total



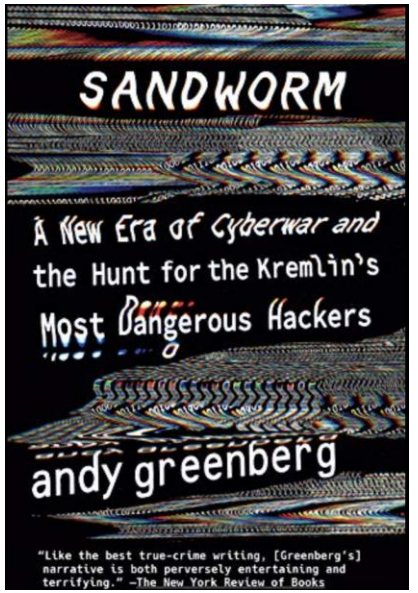
Prior/Projected Commissioning/Career Production

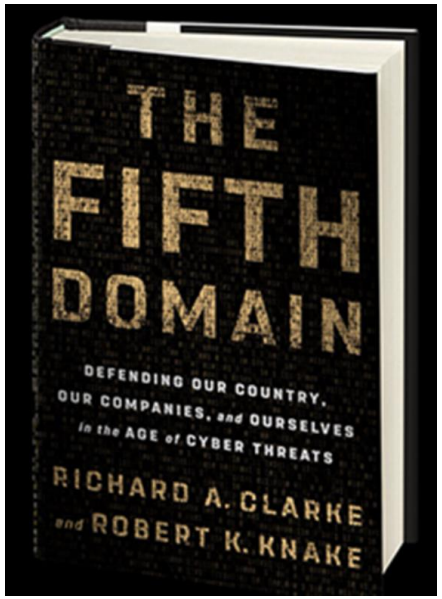


CySER VICEROY to Date

- **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**

- *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

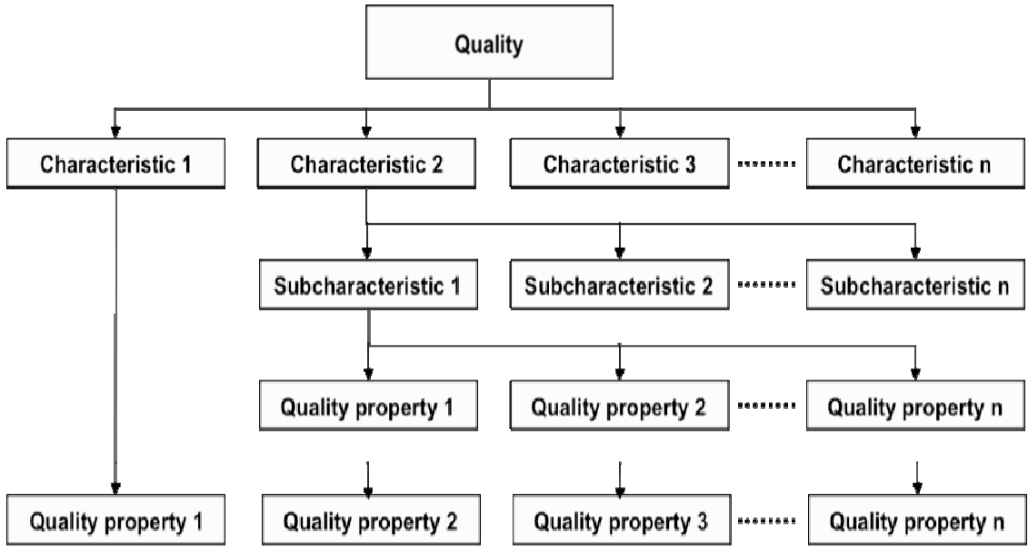
CySER Participants:

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

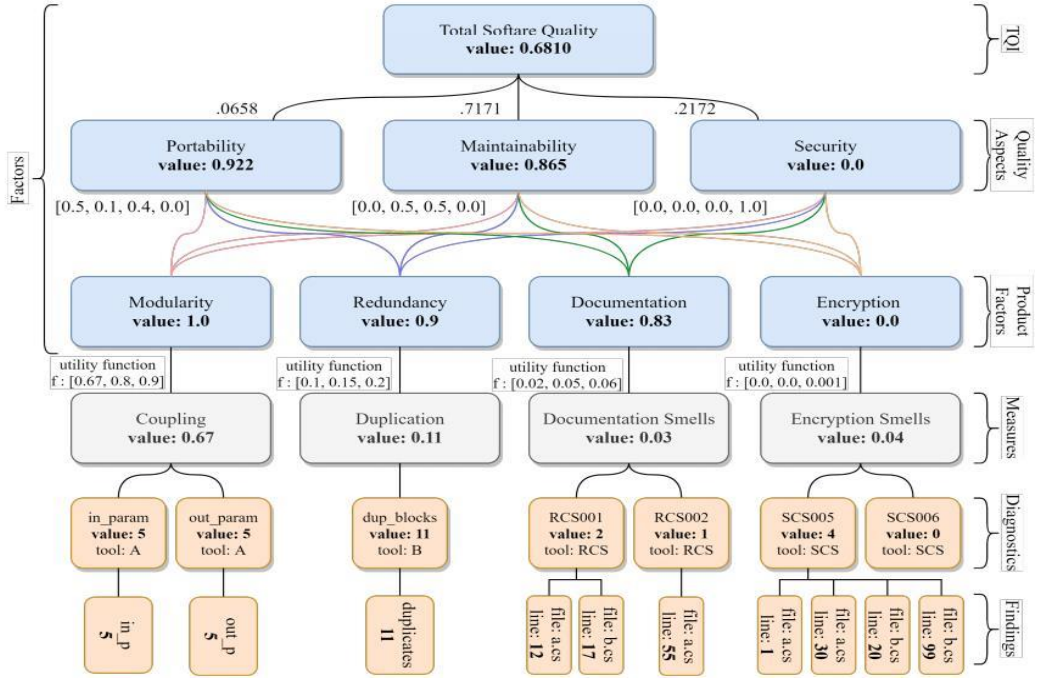
Hierarchical Software QA Modeling

Theoretical



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

Operational



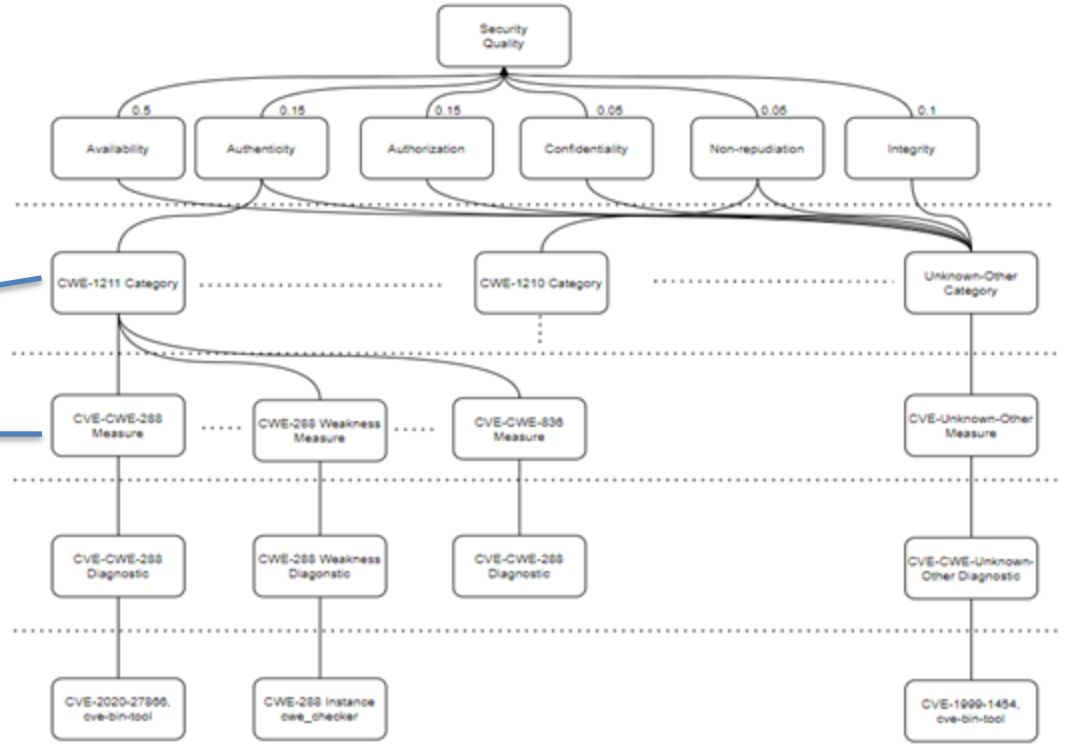
Quamoco (2012 Wagner et al.)
Qatch (2017 Miltiades et al.)
PIQUE (2020 SEL MSU)

CWE-699 View Structure

699 - Software Development
- API / Function Errors - *(1228)*
  - Use of Inherently Dangerous Function - *(242)*
  - Use of Function with Inconsistent Implementations - *(474)*
  - Undefined Behavior for Input to API - *(475)*
  - Use of Obsolete Function - *(477)*
  - Use of Potentially Dangerous Function - *(676)*
  - Use of Low-Level Functionality - *(695)*
  - Exposed Dangerous Method or Function - *(749)*
- Audit / Logging Errors - *(1210)*
  - Improper Output Neutralization for Logs - *(117)*
  - Truncation of Security-relevant Information - *(222)*
  - Omission of Security-relevant Information - *(223)*
  - Obscured Security-relevant Information by Alternate Name - *(224)*
  - Insertion of Sensitive Information into Log File - *(532)*
  - Insufficient Logging - *(778)*
  - Logging of Excessive Data - *(779)*
- Authentication Errors - *(1211)*
  - Authentication Bypass Using an Alternate Path or Channel - *(288)*
  - Authentication Bypass by Spoofing - *(290)*
  - Authentication Bypass by Capture-replay - *(294)*
  - Improper Certificate Validation - *(295)*
  - Improper Following of a Certificate's Chain of Trust - *(296)*
  - Improper Check for Certificate Revocation - *(299)*
  - Incorrect Implementation of Authentication Algorithm - *(303)*
  - Missing Critical Step in Authentication - *(304)*
  - Authentication Bypass by Primary Weakness - *(305)*
  - Missing Authentication for Critical Function - *(306)*
  - Improper Restriction of Excessive Authentication Attempts - *(307)*
  - Use of Single-factor Authentication - *(308)*
  - Use of Password System for Primary Authentication - *(309)*
  - Key Exchange without Entity Authentication - *(322)*
  - Use of Client-Side Authentication - *(603)*
  - Overly Restrictive Account Lockout Mechanism - *(645)*
  - Guessable CAPTCHA - *(804)*
  - Use of Password Hash Instead of Password for Authentication - *(836)*

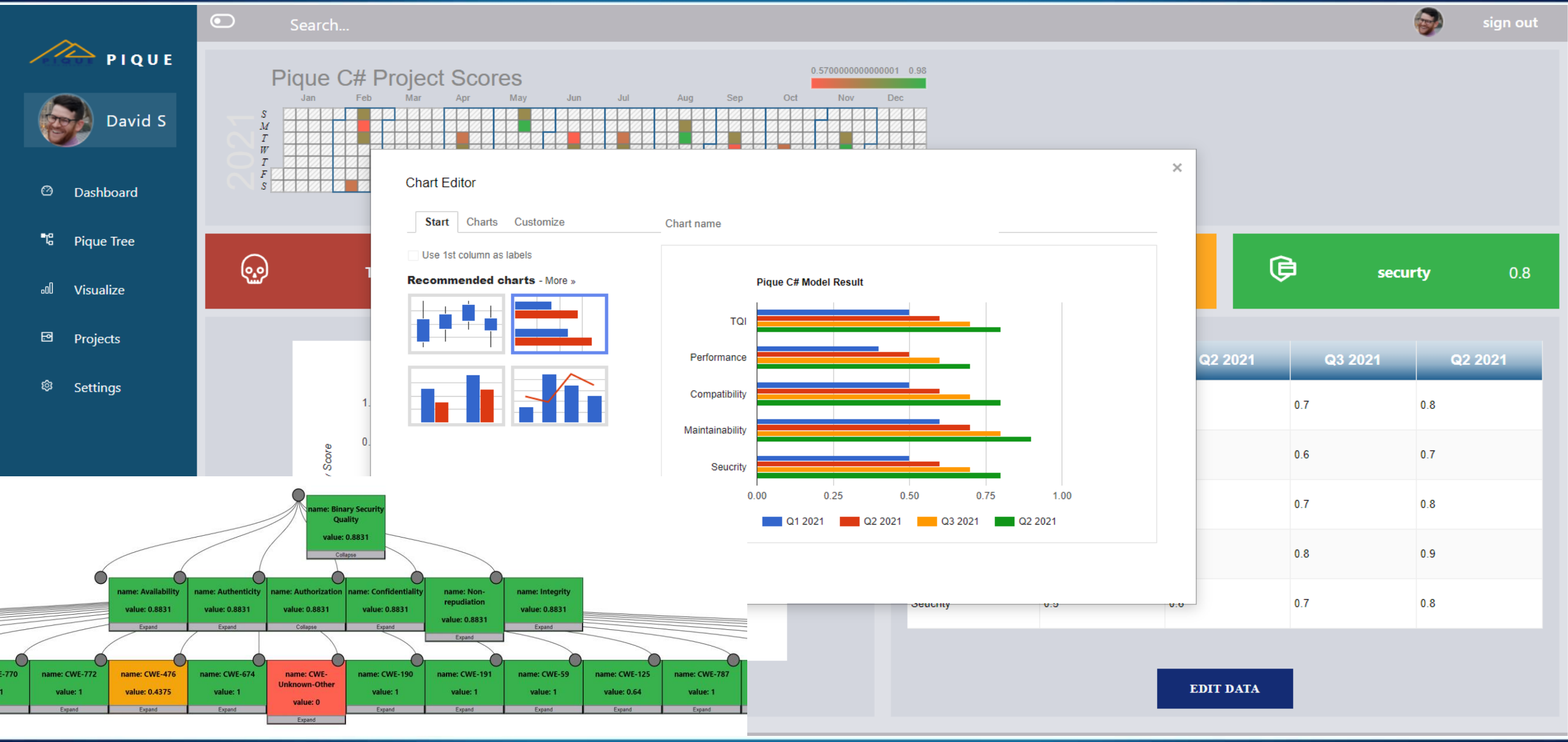
Microsoft STRIDE

	Threat	Property Violated	Threat Definition
S	Spoofing identify	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

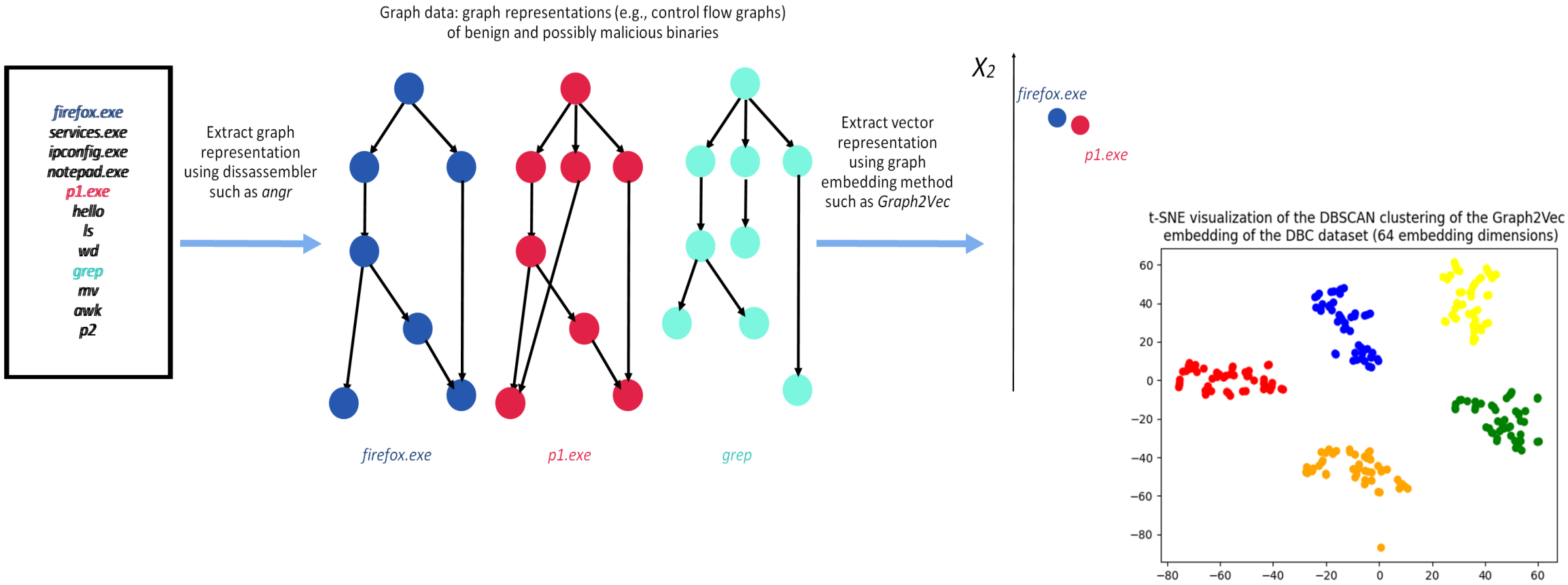


PIQUE Models

- 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)***

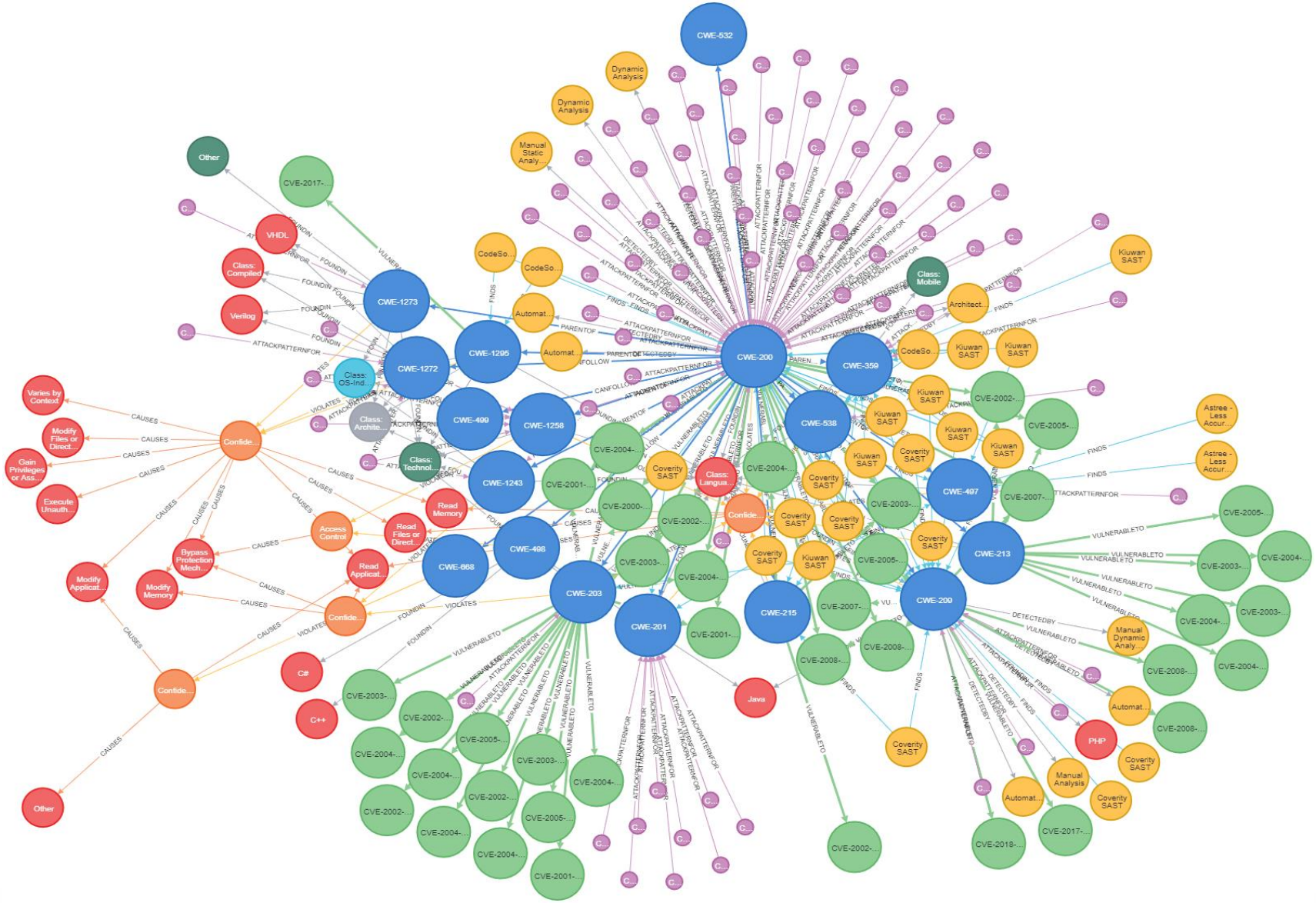

PIQUE
David S
Dashboard
Pique Tree
Visualize
Projects
Settings
Search...
sign out
Pique C# Project Scores
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
2021
Chart Editor
Start
Charts
Customize
Chart name
Use 1st column as labels
Recommended charts - More »
Pique C# Model Result
TQI
Performance
Compatibility
Maintainability
Seucrity
0.00 0.25 0.50 0.75 1.00
Q1 2021 Q2 2021 Q3 2021 Q2 2021
securty 0.8
Q2 2021 Q3 2021 Q2 2021
0.7 0.8
0.6 0.7
0.7 0.8
0.8 0.9
0.7 0.8
EDIT DATA
name: Binary Security Quality value: 0.8831
name: Availability value: 0.8831
name: Authenticity value: 0.8831
name: Authorization value: 0.8831
name: Confidentiality value: 0.8831
name: Non-repudiation value: 0.8831
name: Integrity value: 0.8831
name: CWE-772 value: 1
name: CWE-476 value: 0.4375
name: CWE-674 value: 1
name: CWE-Unknown-Other value: 0
name: CWE-190 value: 1
name: CWE-191 value: 1
name: CWE-59 value: 1
name: CWE-125 value: 0.64
name: CWE-787 value: 1

Classification, clustering, and anomaly detection using graph representations of code

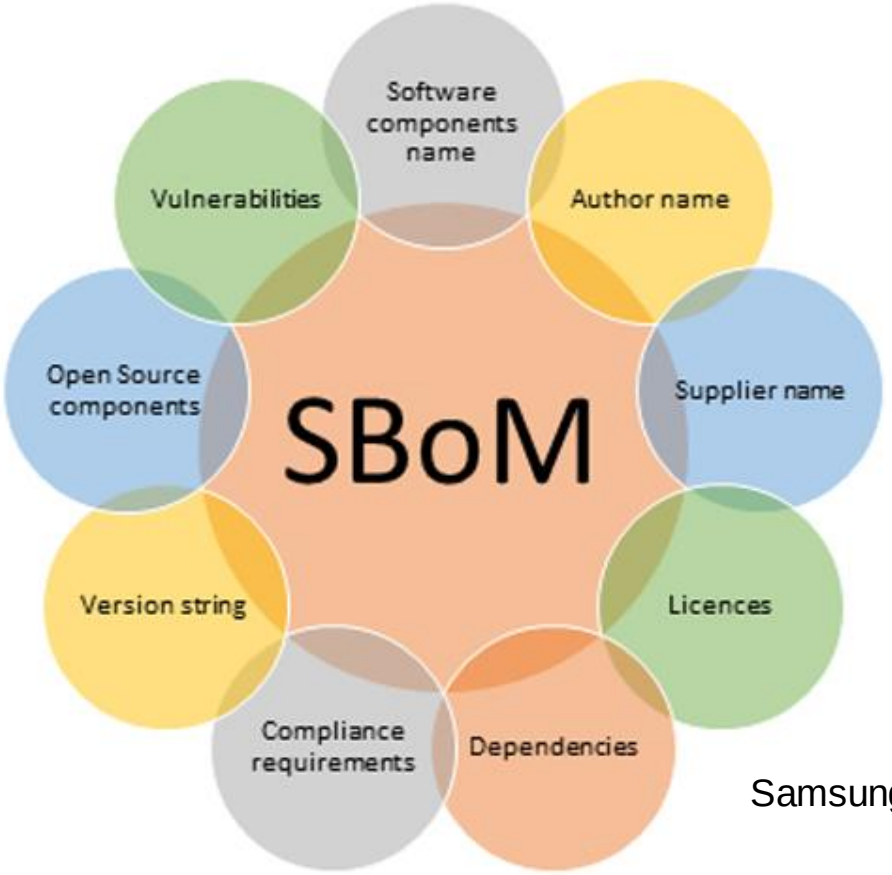


Decomposition of CWE-200

Identify security zones and sensitive sections of source code



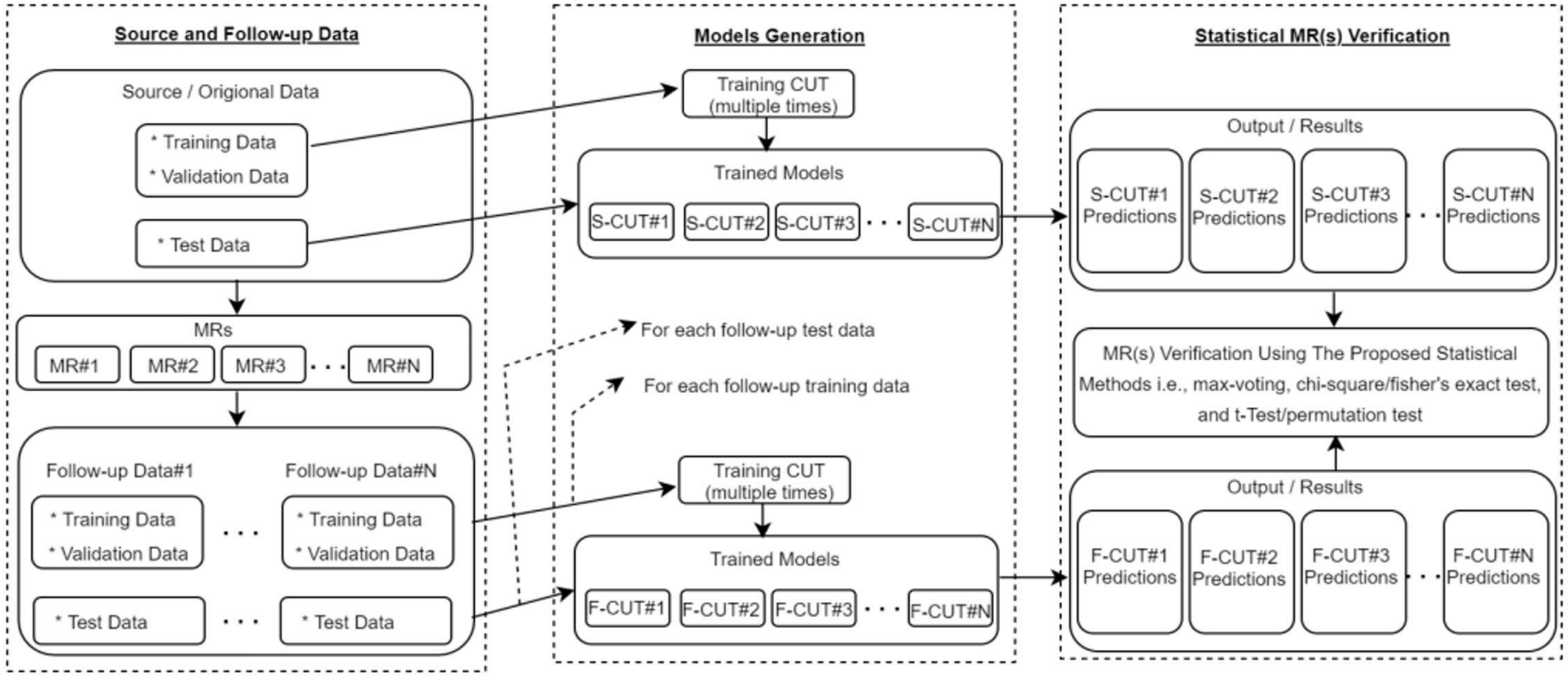
Assess the composition, stylometry and origination of software to verify that they are truthful, complete and accurate



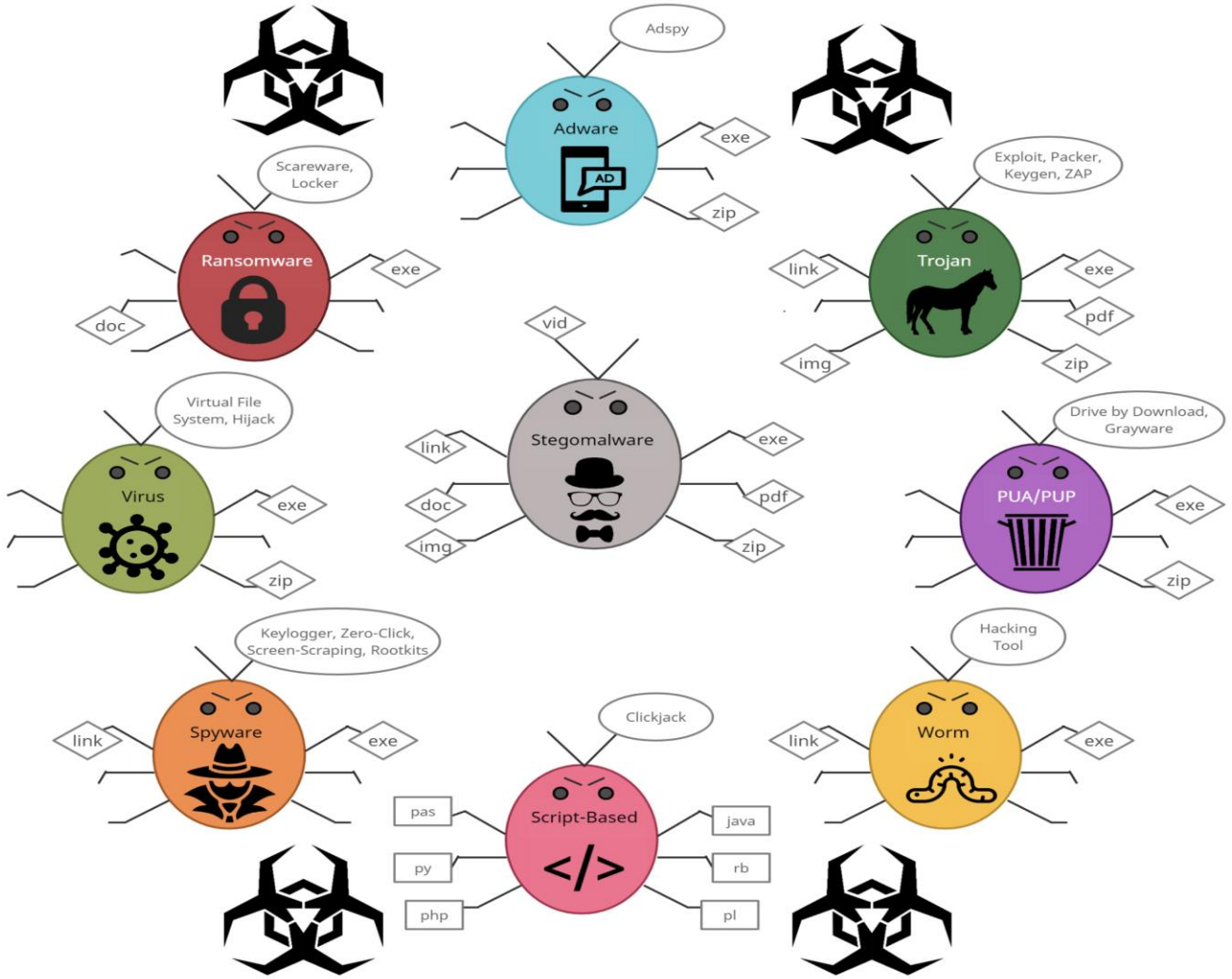
Samsung Research

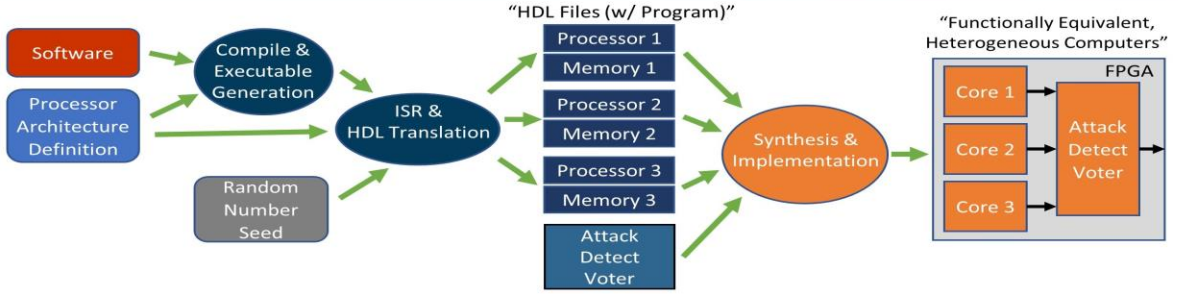
Improving the confidence of machine learning models through improved software testing approaches

Intrusion Detection Systems

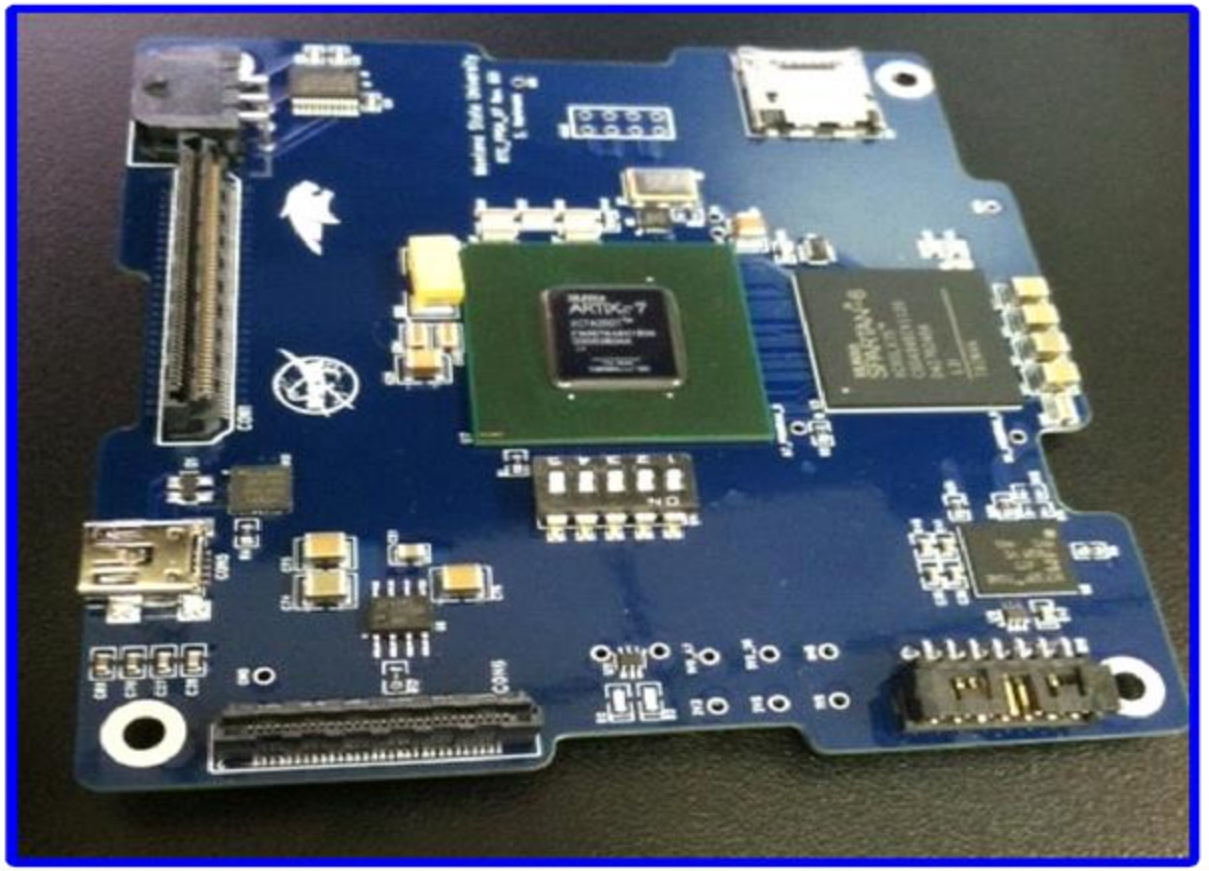


Conceptual Frameworks and Theory of Bug Bounty Platforms





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

Student Projects: Army

Analysis of Cybersecurity's Role in Modern Warfare

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.

Student Projects: Air Force

Darcova Laser + Cyber Component

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.

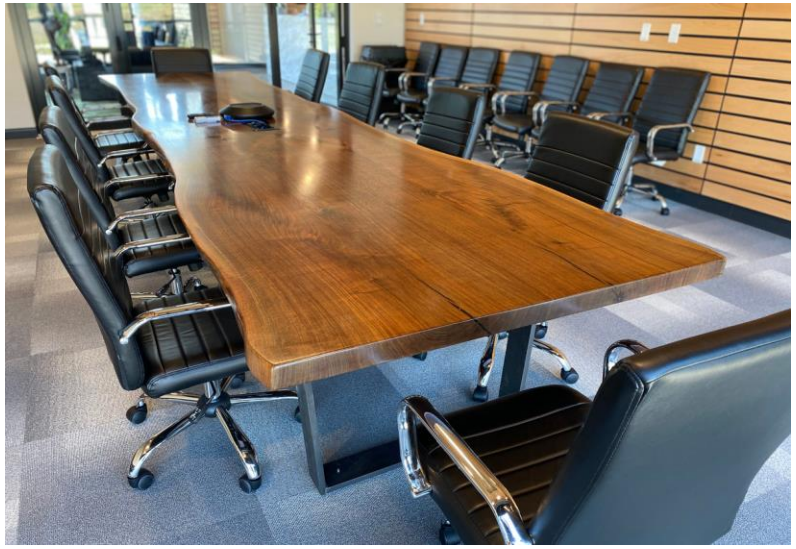
MSU's Applied Research Laboratory

EXPANDING MSU'S ABILITY TO PARTNER WITH INDUSTRY AND GOVERNMENT
TO PROVIDE STUDENTS WITH OPPORTUNITIES IN CLASSIFIED RESEARCH

MONTANA STATE UNIVERSITY
Applied Research Laboratory

ARL FEATURES

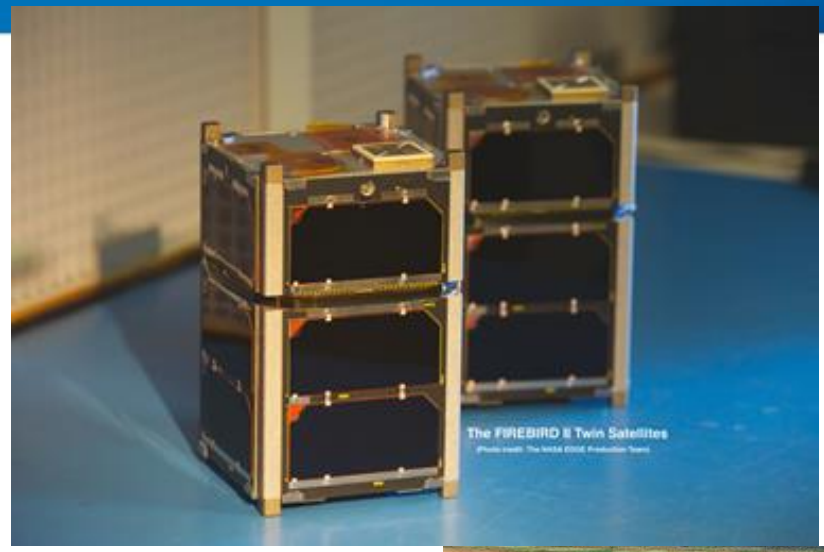
Secure Research Facility



- 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