LA-UR-21-29043

Title:	Cyber Security Summer School 2021
Author(s):	Hsieh Ratliff, Gillian T. Herrera, Grace Annette Moore, Juston Shane
Intended for:	Report
Issued:	2021-09-14

Disclaimer:
Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by Triad National Security, LLC for the National Nuclear Security Administration of U.S. Department of Energy under contract 89233218CNA000001. By approving this article, the publisher recognizes that the U.S. Government retains nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy. Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; as an institution, however, the Laboratory does not endorse the viewpoint of a publication or guarantee its technical correctness.

Cyber Security Summer School 2021

June 2, 2021 - August 6, 2021

School Leads:
Grace Herrera
Gillian Hsieh Ratliff
Juston Moore

Problem Statement and Approach

Why Invest in Cyber Security?

- Cyber security touches every area of information science and technology
  - Information confidentiality, cyber-physical system modeling, adversarial AI, formal software verification, …
- Cyber security is increasingly interdisciplinary, and the challenges are getting harder.
- Cyber security professionals and researchers are in high demand.

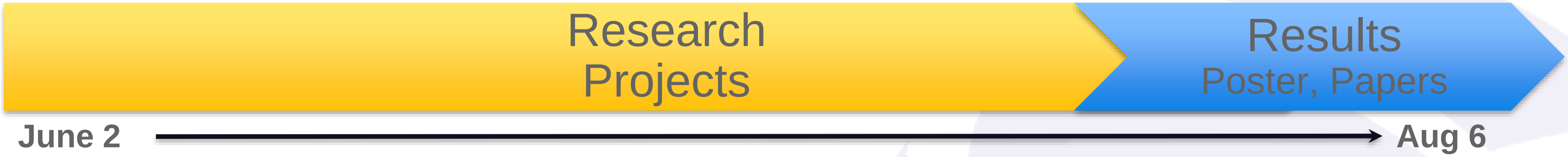
Cyber Security Research and Investigation

- The goal of the **Cyber Toaster: Research Track** is to address emerging national cyber threats.
  - Students conduct projects driven by national needs in: Data Analysis and Anomaly Detection, Control systems and Critical Infrastructure, Adversarial Artificial Intelligence, Cryptography and Formal Methods
- The goal of the **Cyber Toaster: Investigation Track** is to provide participants with the equivalent skills and experience one would obtain working a full month on a professional Incident Response team dealing with an advanced persistent Threat intrusion.
  - Students are trained on the core pillars of incident response: Malware Analysis, Host Forensics, Network Archaeology

Which Divisions / Groups are Most Interested?

- A Division, OCIO, NIE, HPC, WRS-SNA, SSO, T Division, CCS Division.

School Structure



Research Projects

Results

Poster, Papers

June 2 → Aug 6

Investigation Track

- 6 lectures, 8 instructors
  - ○ Week 1: Orientation and Incident Coordination - James Wernicke, Bill Clark
  - ○ Week 2&3: Malware Analysis – Lauren Pearce
  - ○ Week 4: Host Forensics - Chris Rawlings
  - ○ Week 5: Network Archaeology – Neale Pickett
  - ○ Week 6: Operation Technology – Daniel Noyes (INL)
- Analyzing generated data set to create a high level report and technical report/presentation.
  - ○ At the conclusion of the program, students present their findings to senior management in standard incident reporting format.

Research Track

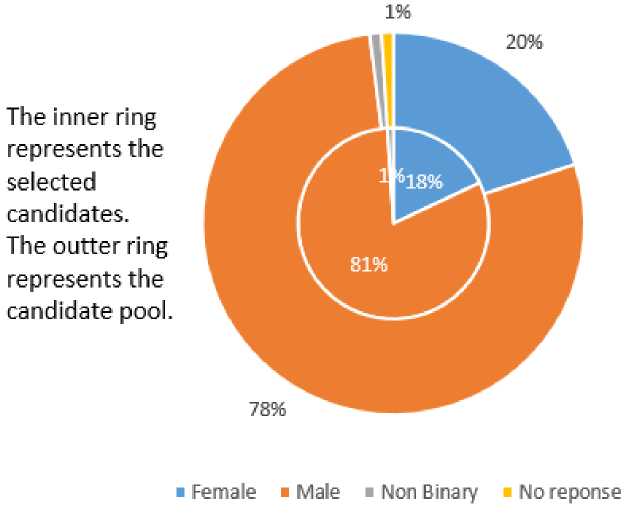
- Students gain experience in communicating their work through posters and oral presentations. In addition, students attend seminars by LANL researchers and external visitors and are given the opportunity to take short courses in core cyber subjects outlined in the Incident Response Track.
- Projects included:
  - ○ cyber analytics (scalable “big data” processing, statistical inference, anomaly detection, deep learning)
  - ○ data integrity (steganography, encryption, adversarial machine learning)
  - ○ intrusion detection and analysis (malware reverse engineering, network/protocol analysis)

Final deliverables: ISTI presentation, Incident Report on findings, presentation to senior management, papers, posters

Selection Process and Demographics

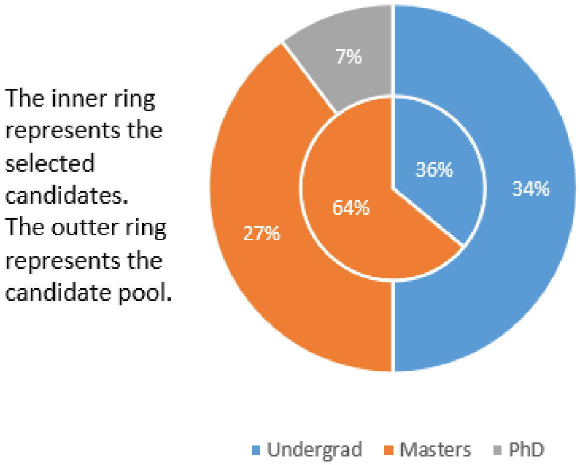
- **Candidate Selection process**
  - Resume committee ranks candidates from 1-5 (mentors include A-4, NIE, T-5, ISR, and T-1)
  - Interview committee - interview the top 10% relevant candidates 1-5 (A-4, NIE, T-5, ISR, and T-1)
  - Selection Criteria
    - Interpersonal skills, Programming/Linux experience, research experience/interest, showed interest in cyber

Gender Candidate Pool vs Seleted Candidate



The inner ring represents the selected candidates. The outter ring represents the candidate pool.

Education Level: Candidate Pool vs Selected Candidate



The inner ring represents the selected candidates. The outter ring represents the candidate pool.

Leadership/Organization

Co-Leads:

- Gillian Hsieh Ratliff (A-4)
- Juston Moore (A-4)
- Grace Herrera (A-4)

Mentors:

Neale Pickett (A - 4)
Grace Herrera (A - 4)
James Wernicke (A - 4)
Lauren Pearce (NIE - ESS)
Chris Rawlings (A-4)
Eric Michalak (A-4)
Aaron Pope(A-4)
Gillian Hsieh Ratliff (A-4)
Heather Keaty (A-4)
Boris Gelfand (A-4)
Juston Moore (A-4)
Michael Dixon (A-4)
Deepjtoti Deka (T-5)
Andrey Lokhov (T-5)
Boian Alexandrov (T-1)
Chris Ren (ISR-3)
Nigel Lawrence (A-4)

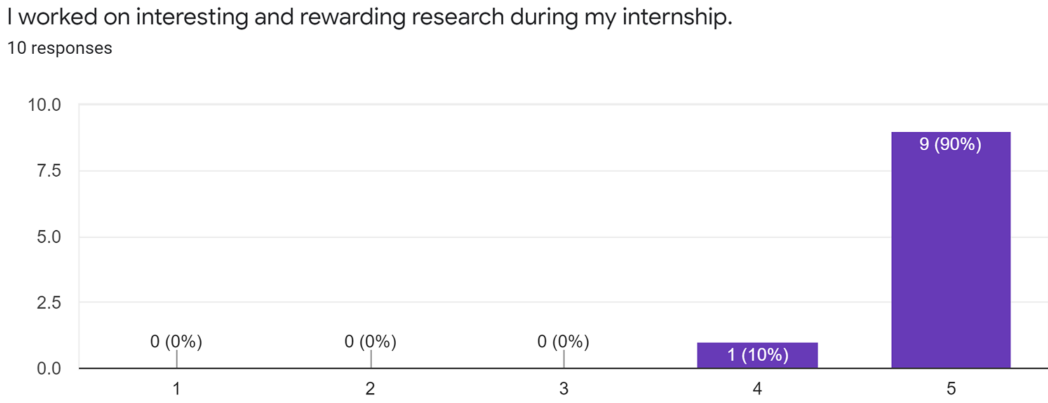
2021 Student Research Projects

Student	Project	Project Outcomes:	Mentor
Sina Sontowski Tennessee Technology University	Detecting Electrical Anomalies via Overlapping Measurements	- Representing LANL in the “DOE Ignite Off!” competition - Plans to publish paper, she will continue to work with her mentors - Presented at the LANL Summer Student Symposium	Nigel Lawrence (A-4) Deepjtoti Deka (T-5)
Jingwen Shi Michigan State University	Learning of Cyber-Physical Systems	- Plans to publish paper, she will continue to work with her mentors	Juston Moore (A-4) Andrey Lokhov (T-5)
Brady Wachs University of Alabama	Generative Image Inpainting with Satellite Images	- Presented at the Cyber Research Track Final Project Presentation	Eric Michalak (A-4) Chris Ren (ISR-3)
Daniel Donze Louisiana State University	Senssembly: Automated Assembly Code Analysis	- Presented at the Cyber Research Track Final Project Presentation	Aaron Pope (A-4) Austin Thresher (A-4)
Dillon Wu Carnegie Mellon University	Yara Rule Generation with Machine Learning	- Presented at the Cyber Research Track Final Project Presentation	Austin Thresher (A-4) Aaron Pope (A-4)
Dani Barrack Portland State University	Secure System Composition and Type Checking using Cryptographic Proofs	- Presented at the LANL Summer Student Symposium - Presented at the Cyber Research Track Final Project Presentation	Michael Dixon (A-4) Boris Gelfand (A-4)
IR Track Students	TF 10 Voting Software Vulnerability	- Presented at the Investigation Track Final Project Presentation	Grace Herrera (A-4), Lauren Pearce (NIE), Chris Rawlings (A-4), Neale Pickett (A-4)

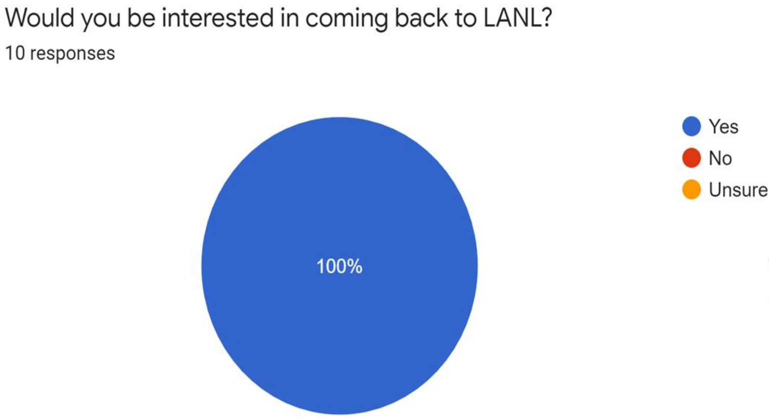
Outcome: Recruiting Record

- **2021 Class (total of 11 students)**
  - Returning Students:
    - Dani Barrack
    - Sina Sontowski
    - Dillon Wu
    - Charles Harper
    - Zachary Leggett
- **2020 Class (total of 12 students)**
  - Returning Students:
    - Maksim Eren, A-4
    - Hans Behren, A-4
    - Deacon Seals, A-4
    - Derek Zhang, CCS-3
- **2019 Class (total of 10 students)**
  - Returning Students:
    - Casey Caruso, Graduate Student
    - Celia Pacheco, Graduate Student
    - Michael Teti, A-4
    - Haydn Jones, A-4
    - Sayera Dhaubhadel, Scientist 1, T-6
- **2018 Class (total of 9 students)**
  - Irene Fang: Post Bachelors Student, XTD-SS
  - Michael Woodham: Aerospace and Defend
  - Charisa Powell: NREL
- **2017 Class (total of 8 students)**
  - Grace Herrera: Scientist 1, A-4
  - Steven Bennett: Post Masters St, A-2
  - Bo Amornrattanapong: Security Professional, NIE-ESS
  - Kyle Buchmiller: Professional, NIE-ESS

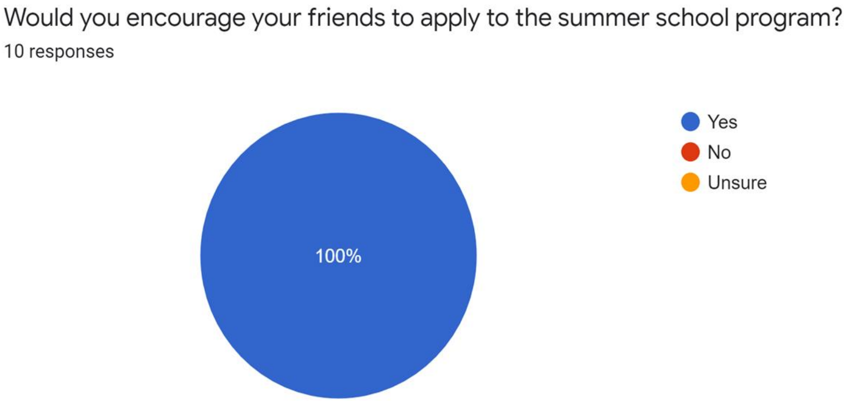
Survey Results


I worked on interesting and rewarding research during my internship.

10 responses


Would you be interested in coming back to LANL?

10 responses


Would you encourage your friends to apply to the summer school program?

10 responses

Student Responses and Feedback

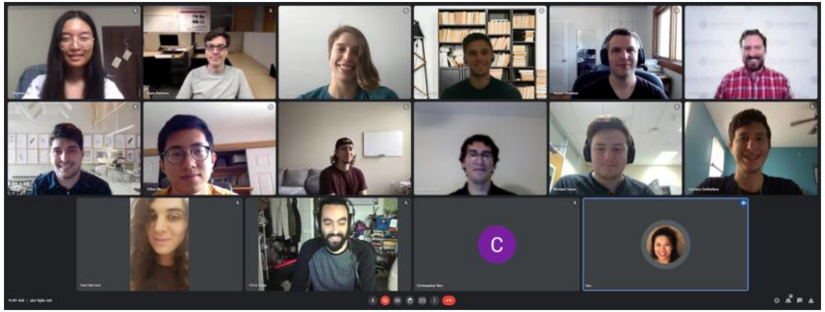
- I appreciated how immediately applicable all the talks were. Everything that was discussed could potentially be implemented in my project and it covered topics that are generally not covered in academic settings.

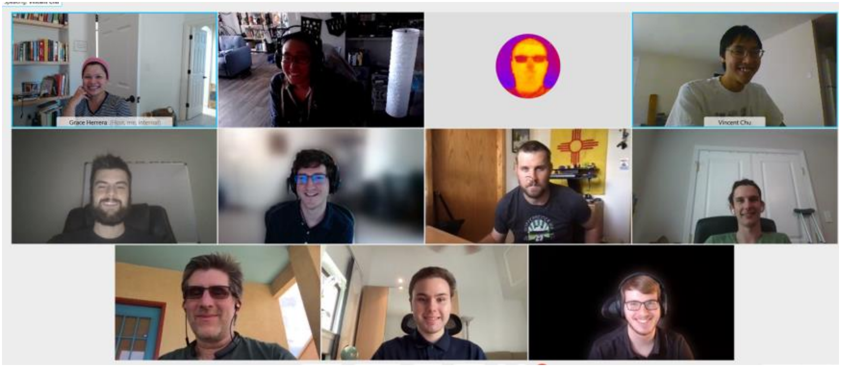
- They offered new perspectives outside of the lab and all had very interesting experiences to share. (on lectures)

- I enjoyed all of the classes a lot, and learned an incredible amount during the 10 week program. It's hard to decide which I enjoyed the most; however, Malware Analysis is something I have been looking forward to learning the longest. It was awesome being exposed to reverse engineering techniques, and I really enjoyed learning about anti-reverse-engineering techniques, and how to get around them. Lauren did an incredible job in explaining reverse engineering, and was readily available to help explain problems we were facing, and how to get better at reverse engineering and malware analysis.

- The general structure of learning and then applying what was learned was great. Attending a lecture to learn a skill (or talking with a mentor or teacher to get help with a skill), then more or less immediately putting it into practice by completing something felt very rewarding. It really offered the opportunity to not only get experience but to have that experience solidified as a part of our skill sets going forward.

Cyber Security School





Cyber Summer School Class of 2021:Investigation Track and Cyber Research Track students with mentors

Project Description

LANL is committed to training the next generation of cyber security professionals and researchers for the US Department of Energy. Alumni are prepared to mitigate rapidly-evolving threats to national security by applying best-practice analysis and developing novel tools.

Project Outcomes

The 2021 summer school ended with another recruiting success, recruiting **5 students into A-4,T, and NIE**-- as staff or students.

- The research track students further strengthened LANL's cyber mission by applying their skills to develop innovative solutions to help address national cyber threats.
  - 1 student was picked to represent LANL in the "DOE Ignite Off!" competition
  - 2 posters in the Student Symposium
  - 2 papers based on student research
- The investigation track students learned the necessary concepts and skills for responding effectively to cyber security incidents.
  - 3 returning students and/or staff
  - Final report and presentation on the generated data set to LANL Management (A-Division, WRS, and SSO) and Sandia National Laboratory

***PI:* Gillian Hsieh Ratliff**

***Total Project Budget:* $350,000.00* (DOE, A-Div, ISTI)**

- **$100,000.00 ISTI**

ISTI Focus Area: Data Science and Artificial Intelligence

END

Self Assessment and Wish List

- **Things that went well**
    - Technical interviews resulted in better quality students overall.
    - Involvement from other groups and labs.
    - Excellent feedback from CSIRT on the quality of the candidates.
    - Having both an IR and Research track was very successful.
    - Received high praise from A-Division management on final presentations.
    - Career panel received positive feedback from students.
- **Things that we plan to improve next year**
    - Include more networking opportunities with staff outside the group and student pool (virtual).
        - we will add more virtual game nights, virtual coffee breaks, and brown bags
        - if in-person we will have coffee breaks, brown bags
    - If we’re able to have an in-person school we will reinstate CSIRT tours and social engagements.
    - We will work with mentors to change timelines and give students longer periods of focused time on final projects.
    - Engage with HR earlier so that the students don’t get conflicting information before the internship starts.
    - Earlier staff engagement with students – month before the internship starts – weekly touchpoints.
- **Things that we would like from ISTI and other sponsors for next year**
    - ISTI tea times were fantastic!
    - We would prefer to receive funding information earlier so that we could make offers and remain competitive.

Students in 2021

Student	University
John Rawley	Florida State University
Zach Leggett	Auburn University
Charles Glass	Louisiana State University and Agricultural and Mechanical College
Charlie Harper	Auburn University
Simon Brucklich	Northeastern University
Daniel Donze	Louisiana State University
Dani Barrack	Portland State University
Brandon Wachs	The University of Alabama
Sina Sontowski	Tennessee Technological University
Dillon Wu	Carnegie Mellon University
Jingwen Shi	Michigan State University