WELCOME

David White

Director, National Security Programs

Sandia National Laboratories
Cybersecurity Research at SNL

Will Zortman
SANDIA’S HISTORY IS TRACED TO THE MANHATTAN PROJECT

In my opinion you have here an opportunity to render an exceptional service in the national interest.

- July 1945
  Los Alamos creates Z Division
- Nonnuclear component engineering
- November 1, 1949
  Sandia Laboratory established
- AT&T: 1949–1993
- Lockheed Martin: 1995–2017
- Honeywell: 2017–present
SANDIA’S BUDGET COVERS A BROAD RANGE OF WORK

**DoD**
- Air Force
- Army
- Navy
- Defense Threat Reduction Agency
- Ballistic Missile Defense Organization
- Office of the Secretary of Defense
- Defense Advanced Research Projects Agency
- Intelligence Community

**OTHER DOE**
- Science
- Energy Efficiency and Renewable Energy
- Nuclear Energy
- Environmental Management
- Electricity Delivery and Energy Reliability
- Other DOE

**OTHER**
- Department of Homeland Security
- Other federal agencies
- Nonfederal entities
- CRADAs, licenses, royalties
- Inter-entity work

**NONPROLIFERATION**
- NNSA/NA20
- State Department

**ACTUAL FY18 BUDGET $3.64B**

- NNSA Weapons: 53.0%
- DoD-Nuclear Deterrence: 6.1%
- Other DoD: 19.6%
- Other DOE: 7.3%
- Other: 7.4%
- Nonproliferation: 6.6%
TECHNOLOGY-BASED ECONOMIC DEVELOPMENT
Helping New Mexico companies start up and grow

New Mexico Small Business Assistance (NMSBA)
- 6,858 new jobs created and retained; all 33 New Mexico counties supported
- $57.9M in technical assistance to 2,797 New Mexico small businesses
- 2017: $2.4M in assistance provided by Sandia alone, 188 small businesses in 21 counties

Sandia Science & Technology Park (SSTP)
- 47 companies and organizations employing 2,059 people
- $384.8M of investment
- $98K average annual salary, $5.4B wages and salaries generated
- 2018: 3 new companies

Entrepreneurial Separation to Transfer Technology (ESTT)
- 162 Sandia entrepreneurs have left the Labs
- 113 companies started up or expanded
- 2018: 5 entrepreneurs left to start 4 companies and expand 1 company

Center for Collaboration and Commercialization (C3) Entrepreneur Exploration (EEx)
- 68 entrepreneur events, 3,319 participants including both Sandians and community members
- C3 location at the University of New Mexico Lobo Rainforest building fosters collaboration with UNM
- 2018: EEx had 22 entrepreneur events with 1,256 participants
SANDIA’S WORKFORCE IS GROWING

Staff has grown by over 3,800 since 2009 to meet all mission needs
OUR PRIORITIES CREATE A VISION FOR THE FUTURE

- Deliver quality engineering, science, and technology in the most efficient way possible
- Safety and security are top of mind
- Collaboration is vital – inside and outside the Labs
- Sustain a diverse and inclusive Laboratories culture
- Think strategically: What might the world look like in 20 to 30 years?
SANDIA ADDRESSES NATIONAL SECURITY CHALLENGES

1950s
- NUCLEAR WEAPONS ENGINEERING AND TESTING
- Arms race

1960s
- NW STOCKPILE DIVERSITY AND BUILD-UP
- Cuban missile crisis & Vietnam War

1970s
- NW + ENERGY: MULTIPROGRAM LABORATORY
- Energy crisis

1980s
- DOE MULTIPROGRAM + MISSILE DEFENSE AND OTHER DoD WORK
- End of Cold War

1990s
- DOE MULTIPROGRAM + DoD, ECONOMIC COMPETITIVENESS
- Stockpile stewardship

2000s
- EXPANDED NATIONAL SECURITY ROLE POST 9/11
- Broader national security

2010s
- MULTIMISSION LAB: LEPs CYBER, BIO, SPACE, TERRORISM
- Evolving national security challenges
SANDIA HAS FIVE MAJOR PROGRAM PORTFOLIOS
Sandia Cyber Centers of Excellence

Enterprise Cybersecurity Defense
- Protecting the Enterprise Network

Civilian Cyber
- Leading critical public-private partnerships

Other US Government Cyber
- Supporting the other government agencies in cyber research
Foundational Infrastructure/Tools

**Foundational**

- Microsystems and Engineering Sciences Applications (MESA) Facilities
- Center for Integrated Nanotechnologies (CINT)
- National Infrastructure Simulation & Analysis Center (NISAC)
- Modeling, simulation & visualization
- Center for Cyber Defenders Student Internship program
Cyber Research Focus Areas

Microelectronic Design and Analysis
Industrial Control System Security
Network Defense
Autonomous Cyber
Big Data and Data Analytics
Software Understanding
Embedded Systems Research
Cyber Modeling and Simulation
Back-Up Slides
Institute Internships

Institute Programs Website

- AutonomyNM
- Center for Computing Research (CCR)
- Interns for Security, Arms Control, and Force Protection Engineering (iSAFE)
- Mathematics & Analytics Research Technical Internship for Advanced National Security (MARTIANS)
- Mission Services Talent Acquisition Team (MSTAT)
- Nonlinear Mechanics and Dynamics (NOMAD)
- Nuclear Weapons Summer Product Realization Institute (NWSPRINT)
- Research and Applications of Mechanics of Structures (RAMS)
- Science of Extreme Environments Research Institute (SEERI)
- SENTINL: Energy Surety Incubator (ESI)
- TITANS: Center for Analysis Systems and Applications (CASA)
- TITANS: Center for Cyber Defenders (CCD)
- TITANS: Interdisciplinary Design, Engineering, and Assurance Students (IDEAS)
- TITANS: Monitoring Systems and Technology Intern Center (MSTIC)
- TITANS: RISE
Post-doc Opportunities

Key areas for post-docs at Sandia:

- Computer science/Computer Engineering
- Electrical Engineering
- Mechanical Engineering
- High-performance computing
- Microelectronics and microfluidics
- Nanotechnology
- Physics
- Chemistry/ Electro Chem
- Biosciences and biotechnology
- Radiation & electrical sciences
- Engineering sciences
- Pulsed power sciences
- Materials science & engineering

Eligibility Criteria

- A recent PhD (conferred 5 years prior to employment) or the ability to complete all PhD requirements before hire date.
What is Emulytics?

Capability to:
- Create model of system of interest (operational or conceptual)
- Create scenarios that transition modeled system into states of interest
  - Architecture, devices, configuration (correct/incorrect), traffic, …
  - Cyber defender scenarios
- Extensive instrumentation for data collection
- Perform analytics on resulting data
- Answer questions about system
Sandia’s Control System Security Research

**Mission:** To reduce the risk of critical infrastructure disruptions due to cyber attacks on control systems.

**Provide decision makers with actionable information**
- Red Team Assessments
- Field Device Analysis
  - PLC monitoring and forensics
  - PLC firmware forensics
  - ICS network detection for ICS traffic
- Emulytics
- Exercise/Test Bed support

**Design resilient systems to withstand cyber-attacks**
- Research next generation security solutions
- Partner with industry to “push” solutions to market
Cybersecurity for Energy Delivery Systems Project Overviews

PRESENTED BY:

Adrian Chavez
adrchav@sandia.gov
505-284-6664
Autonomous Cyber Systems
Sandia National Laboratories
ABOUT YOURSELF

Education
- 2000-2004, B.S. in Computer Science, University of New Mexico
- 2004-2005, M.S. in Computer Science, University of Colorado, Boulder
- 2012-2017, Ph.D. in Computer Science, University of California, Davis

Research Areas
- Cyber security red team assessments
- Code obfuscation
- Moving Target Defense
- Real-time software upgrades
- Cybersecurity for critical infrastructure systems
- Autonomy

Research group interests, size and demographics
- Work focused on cybersecurity for IT/OT systems
- Industry, academic, and government partnerships critical
- > 100 staff in 0582x, and 0588x
- > 10,000 employees at SNL in NM and CA

Keywords:
CURRENT WORK IN CYBERSECURITY

Containerized Application Security for Industrial Control Systems (CAPSec)
- Docker containers to support live-updates and live-migration of software
- Minimize or eliminate any downtime
- Apply towards a microgrid at a partner site
- Partners: Georgia Tech, Fort Belvoir NVESD, Schweitzer Engineering Laboratories, Pacific Northwest National Laboratories, Grimm, Chevron

Survivable Industrial Control Systems
- Automated cyber-physical detection and response within critical infrastructure systems
- Correlate physical events with mod/sim environment and alarm/respond on discrepancies
- Apply towards a microgrid at a partner site
- Partners: Georgia Tech, Fort Belvoir NVESD, Schweitzer Engineering Laboratories, Pacific Northwest National Laboratories, Grimm, Chevron

Alliance
- Combine cyber/physical access control system for Industrial Control Systems (ICS) into a single device
- Red team assessment of prototype
- Partner: Schweitzer Engineering Laboratories
CURRENT WORK IN CYBERSECURITY (cont.)

SDN4EDS
- Document a best-practices guide for deploying Software Defined Networking within ICS environments
- Red team assessment of reference implementation
- Partners: PNNL, Schweitzer Engineering Laboratory, Juniper, SCE, CAISO, Dispersive, USPACOM, and Cisco

Ekhi
- Develop a low-power, low-cost bump-in-the-wire solution for Distributed Energy Resources that can detect/respond to threats
- Apply machine learning algorithms and signature-based intrusion detection systems
- Apply towards emulytics environment
- Partners: OPAL-RT, EPRI

2030 HECO Assessment
- Red team assessment of high-penetration PV system
- Partners: HECO, NREL

Threat Detection & Response
- Distinguish cyber events from physical events in ICS environments
- Machine learning and natural language processing
- Partners: Electric Power Board of Chattanooga, Idaho National Laboratory, Lawrence Berkley National Laboratory, Lawrence Livermore National Laboratory (prime), National Rural Electric Cooperative Association, Oak Ridge National Laboratory, Pacific Northwest National Laboratory, Sandia National Laboratories Schweitzer Engineering Laboratory
FUNDING SOURCES

- Survivable ICS Academic Alliance partnership with Georgia Tech
- CyberForce competition

Department of Energy – Grid Modernization Laboratory Consortium (GMLC)
- Survivable ICS Academic Alliance partnership with Georgia Tech

Department of Energy – Solar Energy Technology Office (SETO)

Department of Homeland Security – Science and Technology

Laboratory Directed Research and Development
RESEARCH NEEDS

Representative IT/OT data to train machine learning algorithms
  ◦ Labeled or unlabeled data

Autonomous cyber security for IT/OT systems
  ◦ Identify
  ◦ Protect
  ◦ Detect
  ◦ Respond
  ◦ Recover

Automated blue team/red team systems to guide secure configuration/deployments of hardware/firmware/software
  ◦ Caldera automated adversary emulation

Partnerships for DOE CEDS and GMLC required
  ◦ Academic partnerships critical
  ◦ Research ideas that have a commercialization path
Questions?

Contact Information:
Adrian Chavez
adrchav@sandia.gov
505-284-6664
Autonomous Cyber Systems
Sandia National Laboratories
Research Spotlight Forum

8.6.19 Cybersecurity

Atomic Precision Advanced Manufacturing

PRESENTED BY:

Shashank Misra, 5229, smisra@sandia.gov
Digital electronics at the atomic limit (DEAL)

Thrust 1: APAM-enabled Devices

- Surface gate
- Donors
- Acceptors
- Doping

Thrust 2: APAM Modeling

- Source
- Gate
- Drain
- Electrons
- Holes

Thrust 3: CMOS Integration

- CMOS
- APAM
- 3 nm

Thrust 4: Application Platform

- Si(100)
- Light
FAIR DEAL GC LDRD

Program Leadership
PI: Shashank Misra
PM: Robert Koudelka
Deputy PM: Rick Muller

#1 APAM-enabled devices
Lead: Shashank Misra

Support Team
Lead: Jennifer Woodrome
Financial: Laurel Taylor
Logistics: Lori Mann
Web: Dorean Chaleunphonh

#2 APAM modeling
Lead: Denis Mamaluy

#3 Integration
Lead: Dan Ward

#4 Application platform
Lead: George Wang

Measurement: Lisa Tracy, Tzu-Ming Lu, David Scrymgeour, Ping Lu, Albert Grine

Microfabrication: Dan Ward, DeAnna Campbell, Mark Gunter, Philip Gamache, Steve Carr, Troy England, Reza Arghavani, Sean Smith

Modeling: Denis Mamaluy, Suzey Gao, Leon Maurer, Andrew Baczewski, Peter Schultz, Quinn Campbell, Juan Granado

Surface Science: Shashank Misra, Ezra Bussmann, George Wang, Aaron Katzenmeyer, Evan Anderson, Scott Schmucker, Esther Frederick, Fabian Pena, Dave Wheeler
APAM creates devices with unique signatures
APAM enables integration of dopants into CMOS late in fabrication flow
Research needs

**Thrust 1: APAM-enabled Devices**

- Surface gate
- Doping
  - Acceptors
  - Donors

**Thrust 2: APAM Modeling**

- Source
- Gate
- Drain
- Electrons
- Holes

**Thrust 3: CMOS Integration**

- CMOS
- APAM

**Thrust 4: Application Platform**

- Si(100)
- Light
Cybersecurity - The Intern Perspective

Presented by:

Michael Reeves, 9315, mreeve@sandia.gov, (reeves17@purdue.edu)
Michael Reeves

- Sandia:
  - Critical Skills Masters Program (CSMP): 9315 Cyber Security Initiatives

- Purdue:
  - Graduated May 2019 Purdue CS undergrad
  - Purdue Masters CS Fall 2020
  - Resident Assistant
  - Sandia SENSE
  - Purdue CCDC team (Collegiate Cyber Defense Competition)

**Keywords:**

Virtualization, Networking, Security
OVERVIEW OF INTERNSHIP AT SNL

• 2 years Sandia Center for Cyber Defenders (CCD)
  • Exposure to upper management
  • Networking Opportunities
  • Tours
  • Tech Talks and workshops

• Projects:
  • Tracer FIRE
  • Kernel Module Testing framework
  • Memory Analysis Tool creation
Outside of Work

- Outside of work:
  - Breweries and Food
  - Climbing and adventures
  - Meow Wolf, Museums and other attractions
  - Volunteering events
Questions?