SAND2015-0977PE

Alex Roesler, Ph.D.

Information Systems Analysis Center

Sandia National Laboratories

Today's National Labs: A Unique Career in National Security and Technology

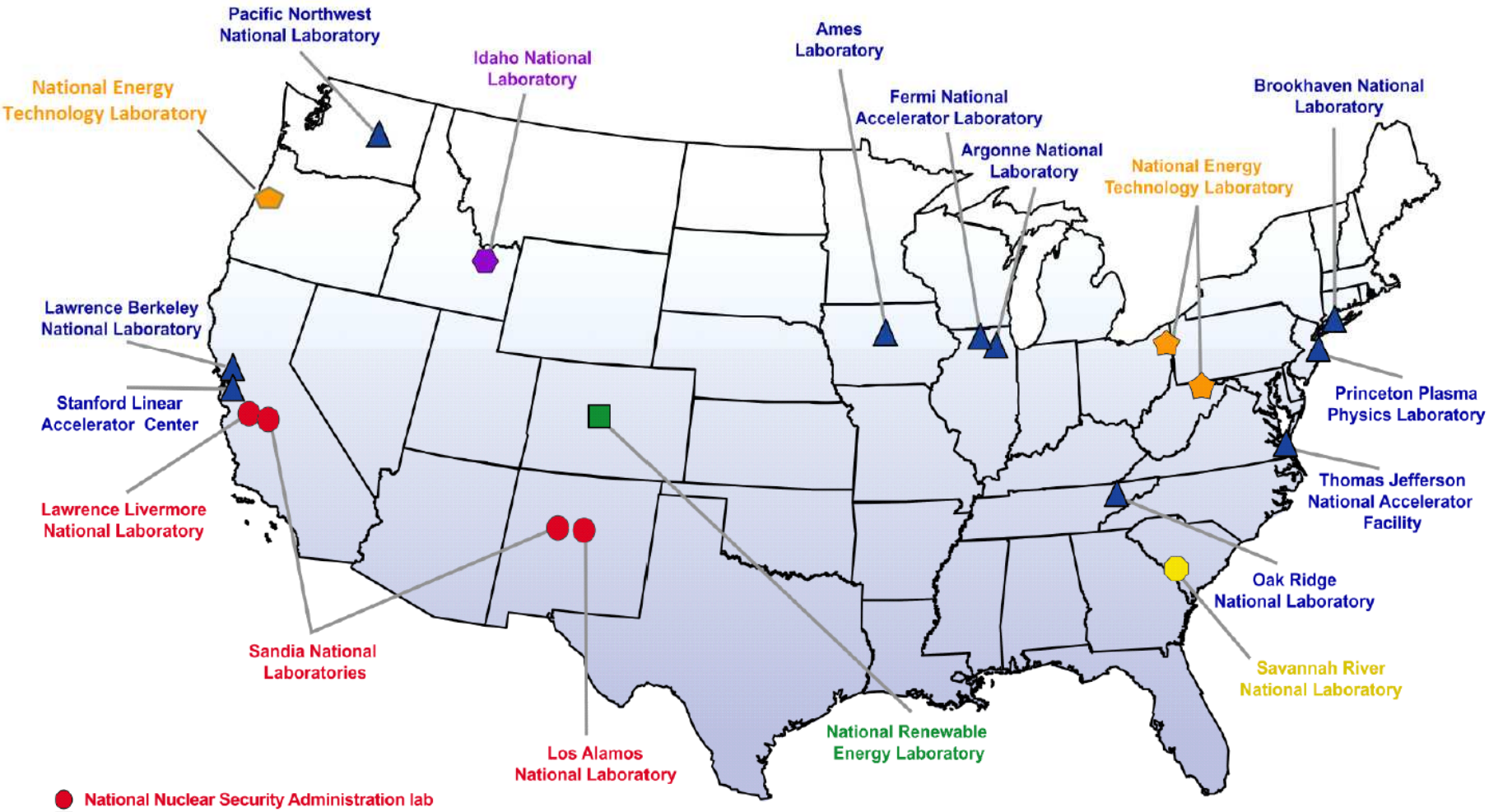
Outline

- National Laboratories Overview
- Who is Sandia National Laboratories
- Background on the evolving cyber threat
- A few cyber technologies we are likely to see in the next 5-10 years
- Opportunities:
  - Technical Internships to Advance National Security (TITANS)
  - Critical Skills Master's Program (CSMP)

Outline

- National Laboratories Overview
- Who is Sandia National Laboratories
- Background on the evolving cyber threat
- A few cyber technologies we are likely to see in the next 5-10 years
- Opportunities:
  - Technical Internships to Advance National Security (TITANS)
  - Critical Skills Master's Program (CSMP)

The Department of Energy Laboratory Complex



Located across 14 states and employing 30,000 scientists

The National Lab System

- The National Lab System invents, builds, and operates one-of-a-kind research facilities and specialized equipment found nowhere else.
- These unique facilities are made available to science, technology and innovation communities from across the nation.
- These facilities, which include powerful X-ray light sources, nanoscience centers and electricity transmission grid test ranges, are more than a national resource for discovery. They are the foundries of future technologies, occupying an experimental niche that universities and the profit-driven private sector can not match.

DOE maintains 16 of the 17 National Labs as GOCOs

- GOCO (Government Owned/Contractor Operated) laboratories are owned by the Government, but managed by contractors.
- GOCO researchers are not Federal employees and have more freedom than GOGO scientists. GOCO employees can assert copyrights, consult with industry, and participate in start-ups based on technology developed at the laboratory.

National Lab Characteristics

- A commitment to their prime sponsor and the original intent of their charter, and to the objectives of their prime sponsoring agency.
  - The mission success of their prime sponsor remains their highest priority.

National Lab Characteristics (cont'd)

- Facilities to address long-term, large-scale problems
  - National Labs address complex technical challenges that often require high risk experiments and large facilities, such as supercomputers or light sources, which are beyond the scale or role of purely academic or commercial entities.
  - Broad, interdisciplinary teams tackle problems that are beyond the scope of university professors or departments.

National Lab Characteristics (cont'd)

- Continuity of expertise
  - Thriving National Labs have maintained technical excellence in critical technical areas, sometimes attracting new or additional sponsors in order to maintain this expertise.
  - In addition to providing successful missions, this continuity fosters an environment that attracts and retains a loyal and highly technical workforce.

Evolving Role of National Labs

- Over the decades since their inception, National Labs have become more diverse in response to expanding national security needs.
- National security missions of the DOE sites include the unique critical skills and capabilities beyond LLNL, LANL and SNL.
- Key work is conducted at:
  - Pacific Northwest National Lab, Oak Ridge National Lab, Argonne National Lab, Idaho National Lab, Brookhaven National Lab, Savannah River Site, Lawrence Berkeley National Laboratory, New Brunswick Lab

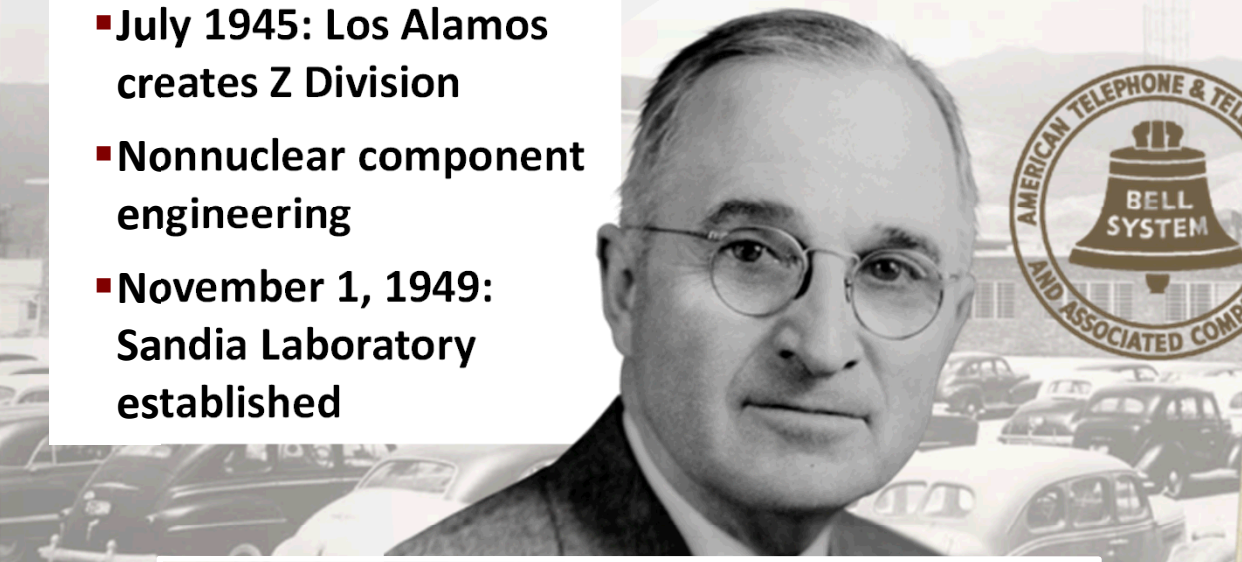
Outline

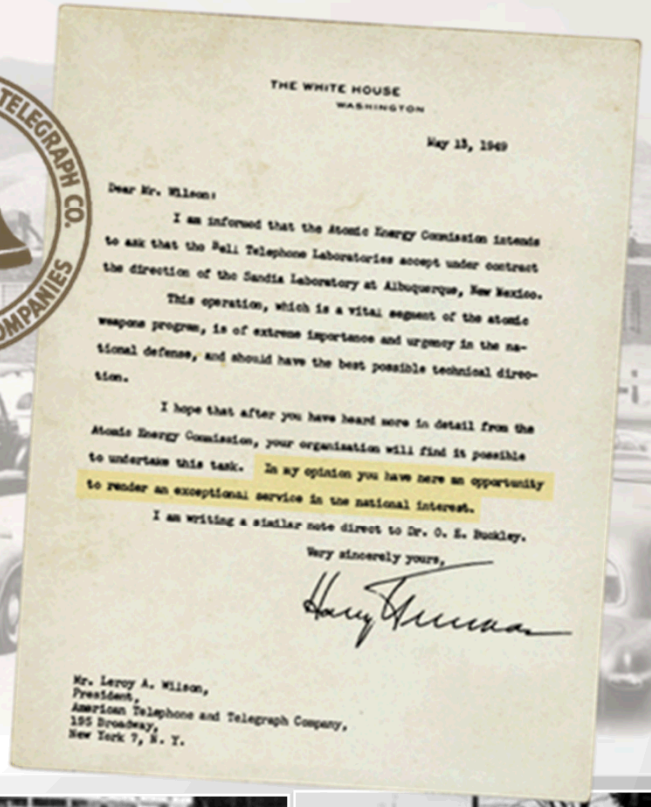
- National Laboratories Overview
- Who is Sandia National Laboratories
- Background on the evolving cyber threat
- A few cyber technologies we are likely to see in the next 5-10 years
- Opportunities:
  - Technical Internships to Advance National Security (TITANS)
  - Critical Skills Master's Program (CSMP)

Sandia's History

Exceptional service in the national interest

- July 1945: Los Alamos creates Z Division
- Nonnuclear component engineering
- November 1, 1949: Sandia Laboratory established





THE WHITE HOUSE
WASHINGTON

May 13, 1949

Dear Mr. Wilson:

I am informed that the Atomic Energy Commission intends to ask that the Bell Telephone Laboratories accept under contract the direction of the Sandia Laboratory at Albuquerque, New Mexico.

This operation, which is a vital segment of the atomic weapons program, is of extreme importance and urgency in the national defense, and should have the best possible technical direction.

I hope that after you have heard more in detail from the Atomic Energy Commission, your organization will find it possible to undertake this task. In my opinion you have here an opportunity to render an exceptional service in the national interest.

I am writing a similar note direct to Dr. O. E. Buckley.

Very sincerely yours,

Harry Truman

Mr. Leroy A. Wilson,
President,
American Telephone and Telegraph Company,
195 Broadway,
New York 7, N. Y.

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

National Laboratories

Two Major Laboratory Sites Anchor Our Set of Distributed Facilities

Albuquerque, New Mexico

Kauai Test Facility, Hawaii

Tonopah Test Range, Nevada

Yucca Mountain, Nevada

WIPP, New Mexico

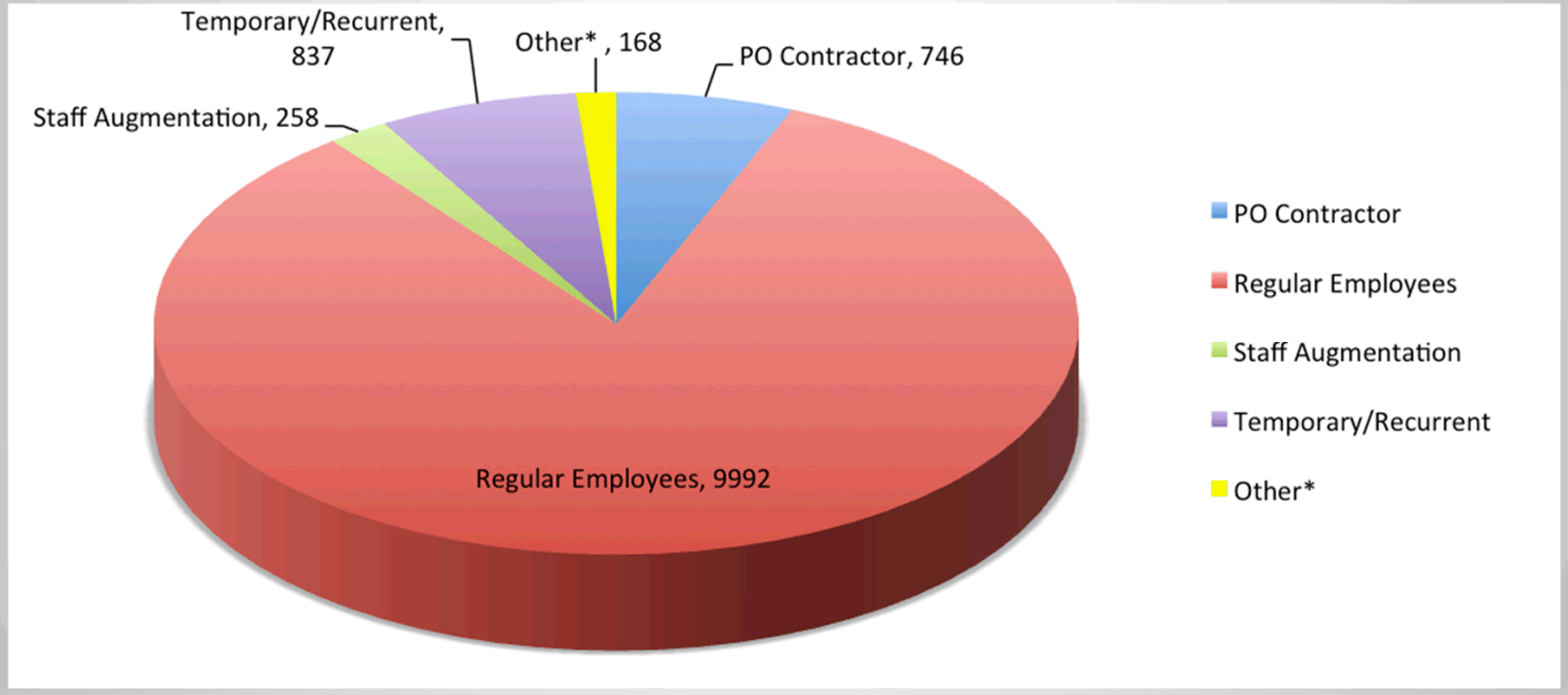
Pantex, Texas

Livermore, California

Our Workforce

- Total Sandia workforce: 12,001
- Regular employees: 9,992
- Advanced degrees: 5,483 (55%)

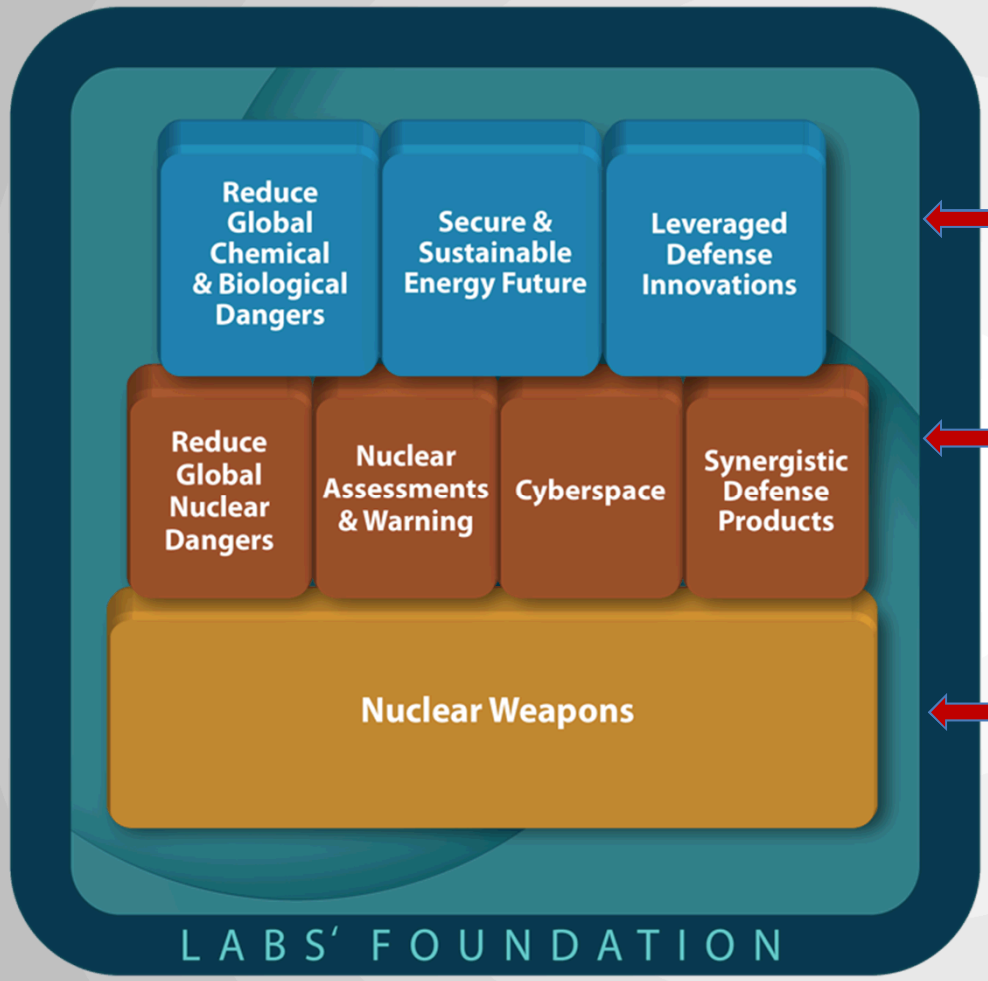
Data as of September 30, 2014



Sandia Addresses Evolving and Expanding National Security Challenges

1950s	1960s	1970s	1980s	1990s	2000s	2010s
Nuclear weapons	Development engineering	Multiprogram laboratory	Missile defense work	Post–Cold War transition	START Post 9/11	LEPs Cyber, biosecurity proliferation
Production and manufacturing engineering	Vietnam conflict	Energy crisis	Cold War	Stockpile stewardship	National security	Evolving national security challenges

National Security Mission Areas

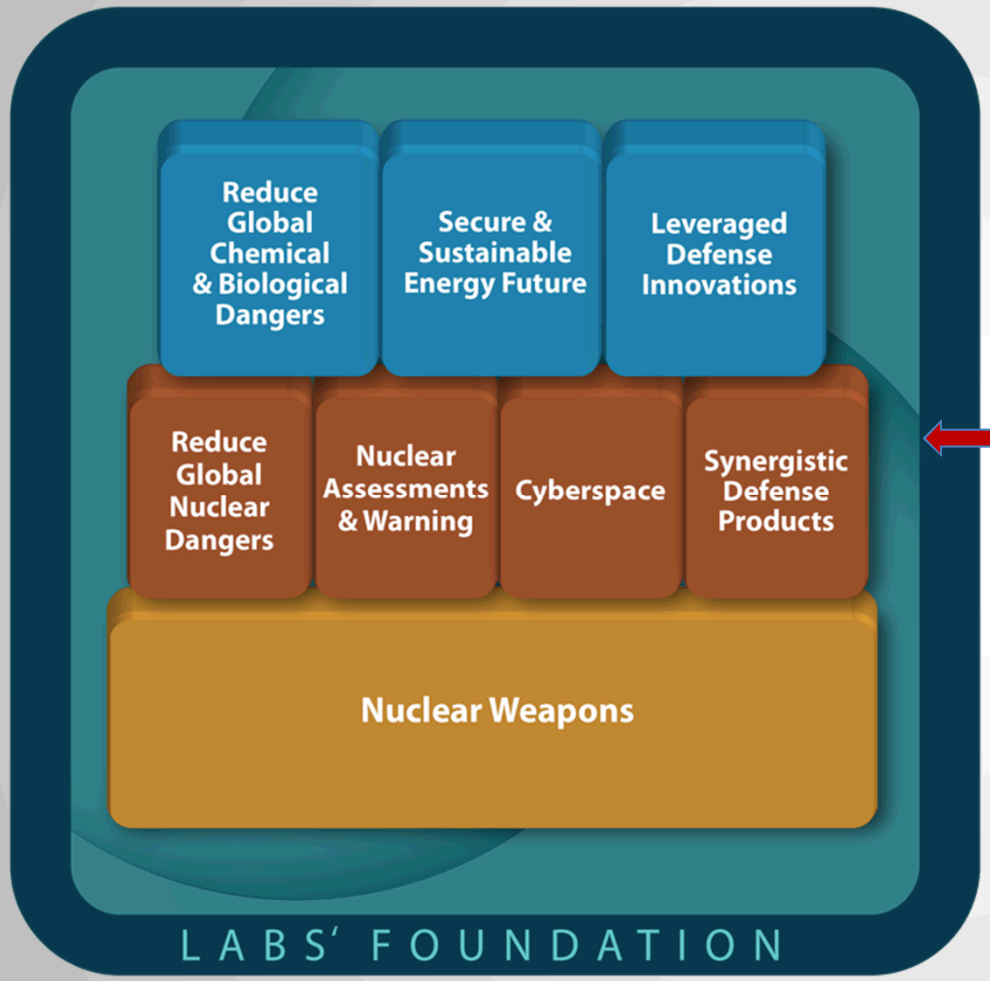


- Top row: Critical to our national security, these three mission areas leverage, enhance, and advance our capabilities.
- Middle row: Strongly interdependent with NW, these four mission areas are essential to sustaining Sandia's ability to fulfill its NW core mission.
- Bottom row: Our core mission, nuclear weapons (NW), is enabled by a strong scientific and engineering foundation.

Sandia's Nuclear Weapons Mission

- Maintain the current U.S. nuclear weapons stockpile
  - Annual Assessment, Surveillance, Limited Life Component Exchanges, Significant Finding Investigations
- Sustain the stockpile into the future
  - Life Extension Programs, Alterations, technology maturation
- Steward the long-term vitality of our capabilities, infrastructure and operations
  - Persistent commitment to multi-disciplinary staff, state-of-the-art labs, equipment, facilities and safe/secure/quality/affordable operations

National Security Mission Areas



- Middle row: Strongly interdependent with NW, these four mission areas are essential to sustaining Sandia's ability to fulfill its NW core mission.

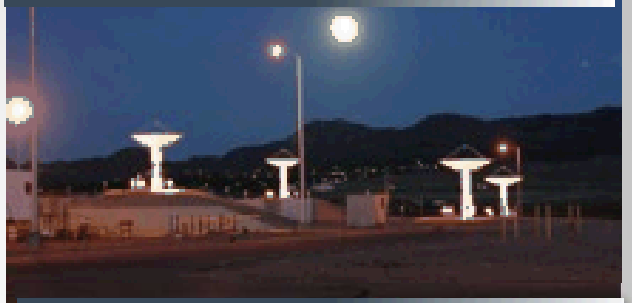
Sample Near Core Activities

Information Operations

Surveillance & Reconnaissance

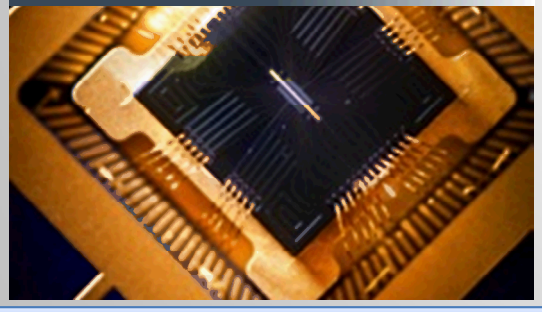
Remote Sensing and Verification

Space Mission



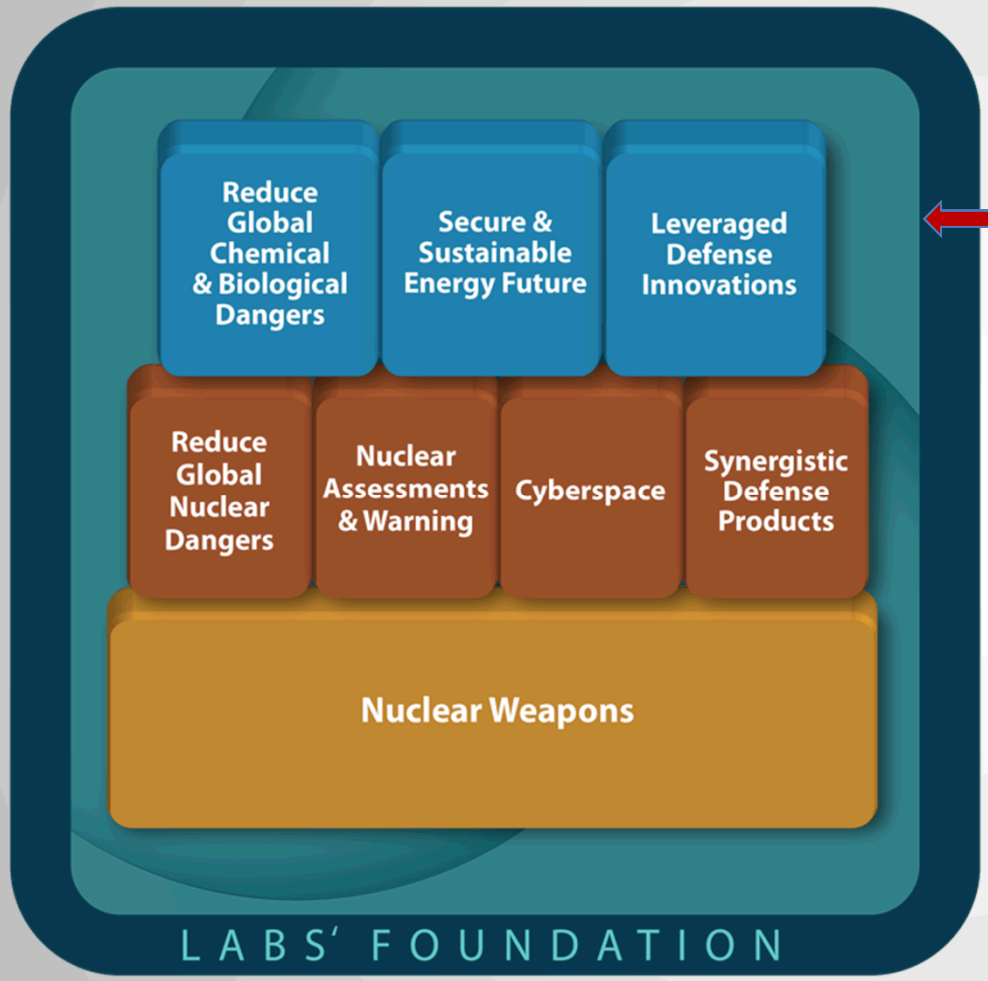
Nuclear Security

Science & Technology Products



Integrated Military Systems

National Security Mission Areas



- Top row: Critical to our national security, these three mission areas leverage, enhance, and advance our capabilities.

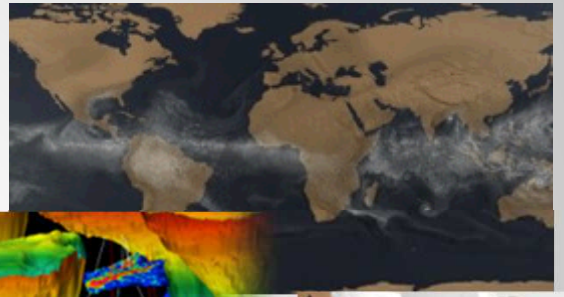
Energy & Climate

Energy Research

ARPAe, BES Chem Sciences, ASCR, CINT, Geo Bio Science, BES Material Science

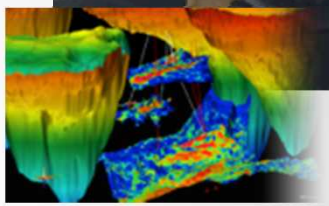
Climate & Environment

Measurement & Modeling, Carbon Management, Water & Environment, and Biofuels



Nuclear Energy & Fuel Cycle

Commercial Nuclear Power & Fuel, Nuclear Energy Safety & Security, DOE Managed Nuclear Waste Disposal

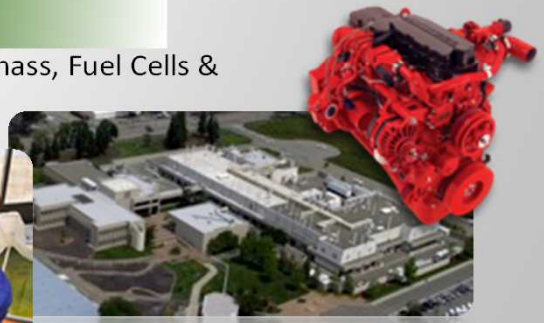


Renewable Systems & Energy Infrastructure

Renewable Energy, Energy Efficiency, Grid and Storage Systems

Transportation Energy & Systems

Vehicle Technologies, Biomass, Fuel Cells & Hydrogen Technology



Sandia National Laboratories

Reduce Global Chem & Bio Dangers

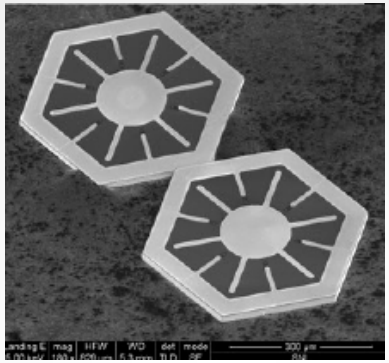
Weapon Remediation

Counterterrorism and Response

Unique Facilities:

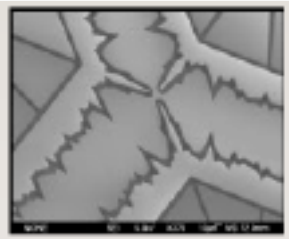
Microsystems & Engineering Sciences Applications (MESA) Complex

- Radiation-hardened microelectronics
- MEMS devices
- "Solar glitter"
- Novel biological and chemical microsensors
- Quantum physics based devices



Microsystems Enabled Photovoltaics

MESA combines silicon processing, packaging and integration, and fabrication of compound-semiconductor devices under one roof.



Ion Trap

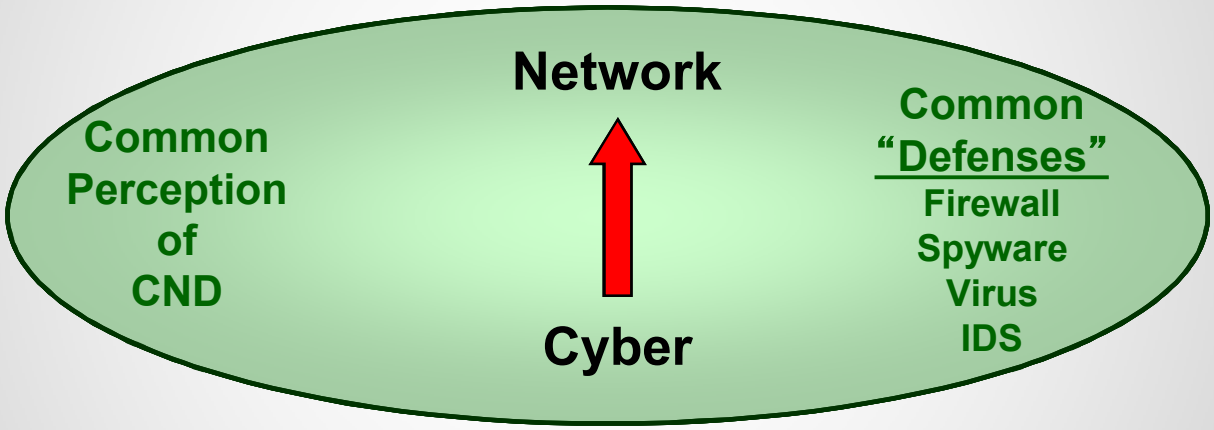
Working at a National Lab: A Unique Career

- Diverse mission areas and a deep commitment to mission success and technical excellence
- Outstanding lifelong learning and development opportunities
- The opportunity to work in or with unique world-class research facilities
- Continuity: 25+ year careers are the norm, not the exception

Outline

- National Laboratories Overview
- Who is Sandia National Laboratories
- Background on the evolving cyber threat
- A few cyber technologies we are likely to see in the next 5-10 years
- Opportunities:
  - Technical Internships to Advance National Security (TITANS)
  - Critical Skills Master's Program (CSMP)

The Common Misconception of Computer Network Defense (CND)

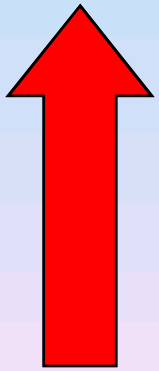


The Real Problem of Computer Network Defense (CND)

Hardware and Software

SCADA	Weapons	Network	C2	Logistics	Storage

Defender must be successful everywhere, continuously, and frequently in the open



Full Spectrum of Offensive Tools

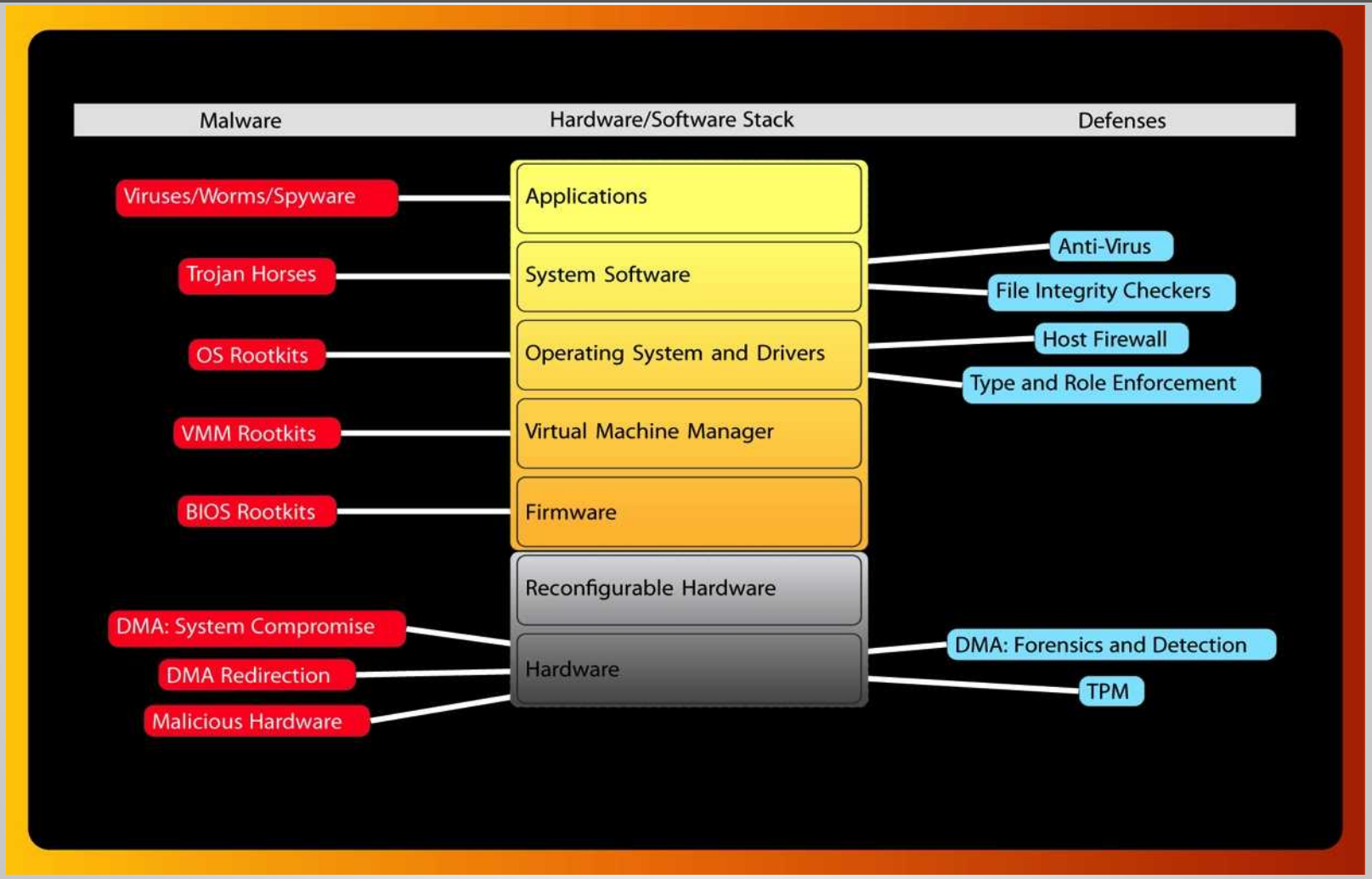
Entry	Human	Sigint	ClanTech	Cyber	Special	Liaison	Deception	Cover Company

Adversary Determines the Time, Place, Combination of Methods and Operates in Secrecy

Threat Model

- Sophisticated adversaries influence commercial hardware and software supply chains
- Sophisticated adversaries have ongoing access to systems through administration, configuration, and updates
- Sophisticated adversaries exploit complexity
- Sophisticated adversaries rely on limits to deeply inspect systems and detect unauthorized activity

Malware and Defenses

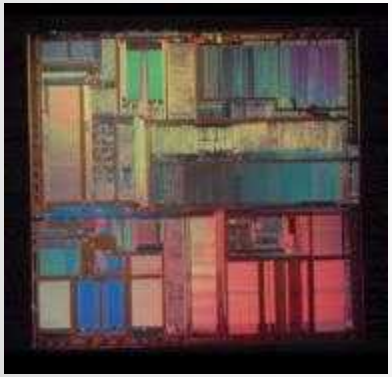


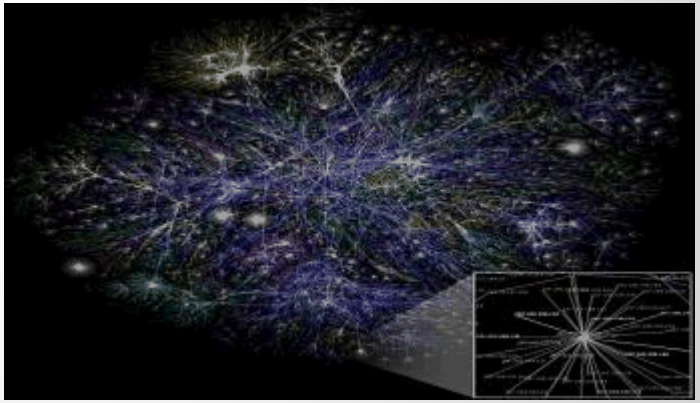
The problem: we can't trust our machines and we can't live without them.

Information systems have become too complex and too interconnected at all scales to ensure that they do not contain vulnerabilities.

- Multi-scale: micro (3 lines of code) -> human -> macro (Internet)
- Multi-discipline: device physics -> electronics -> computer architecture -> software -> human factors
- Multi-medium: photons -> electrons -> RF

- Wafer
- Mask
- Programming
- Die



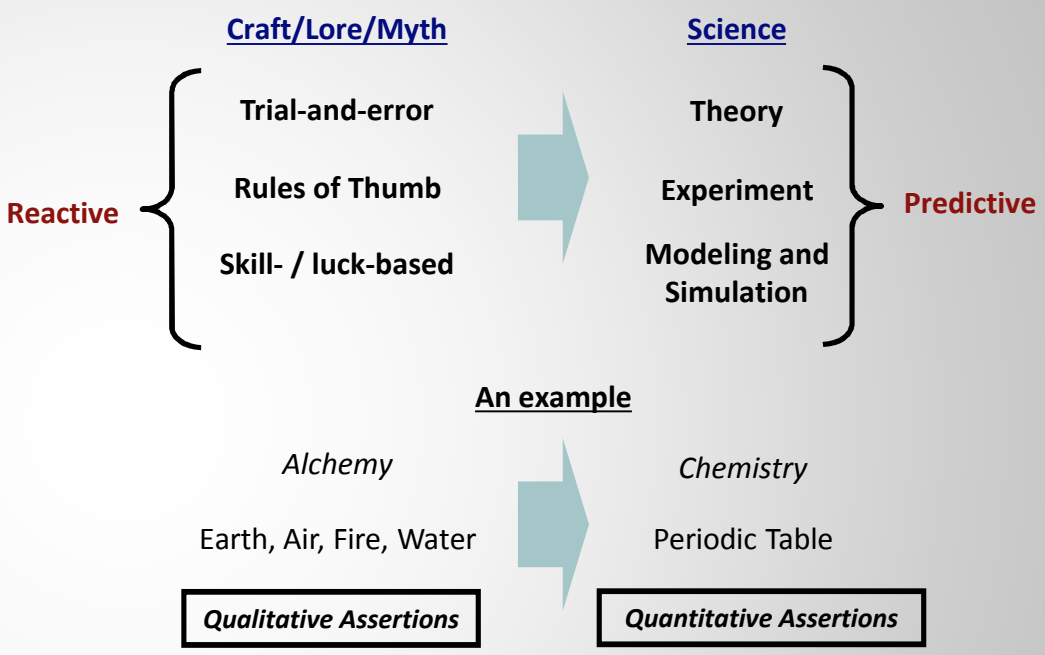


- Servers
- Routers
- Switches
- Fiber
- Firewalls
- Desktops
- Users

…we are behind and falling further behind.

We Need Cost Effective Disruptive Security Technologies

- Our mind set needs to shift - assume that the adversary is in our networks
- We have to significantly raise the cost equation for the adversary
- We have to increase "penalties" for illegal access
- We need to move cyber security from a craft/lore/myth to a scientific discipline.



Outline

- National Laboratories Overview
- Who is Sandia National Laboratories
- Background on the evolving cyber threat
- A few cyber technologies we are likely to see in the next 5-10 years
- Opportunities:
  - Technical Internships to Advance National Security (TITANS)
  - Critical Skills Master's Program (CSMP)

What can we expect in the next five to ten years for Cyber?

Here are three:

- Dynamic Authentication
- Randomness / Diversity
- WeaselBoard (a Sandia technology…)

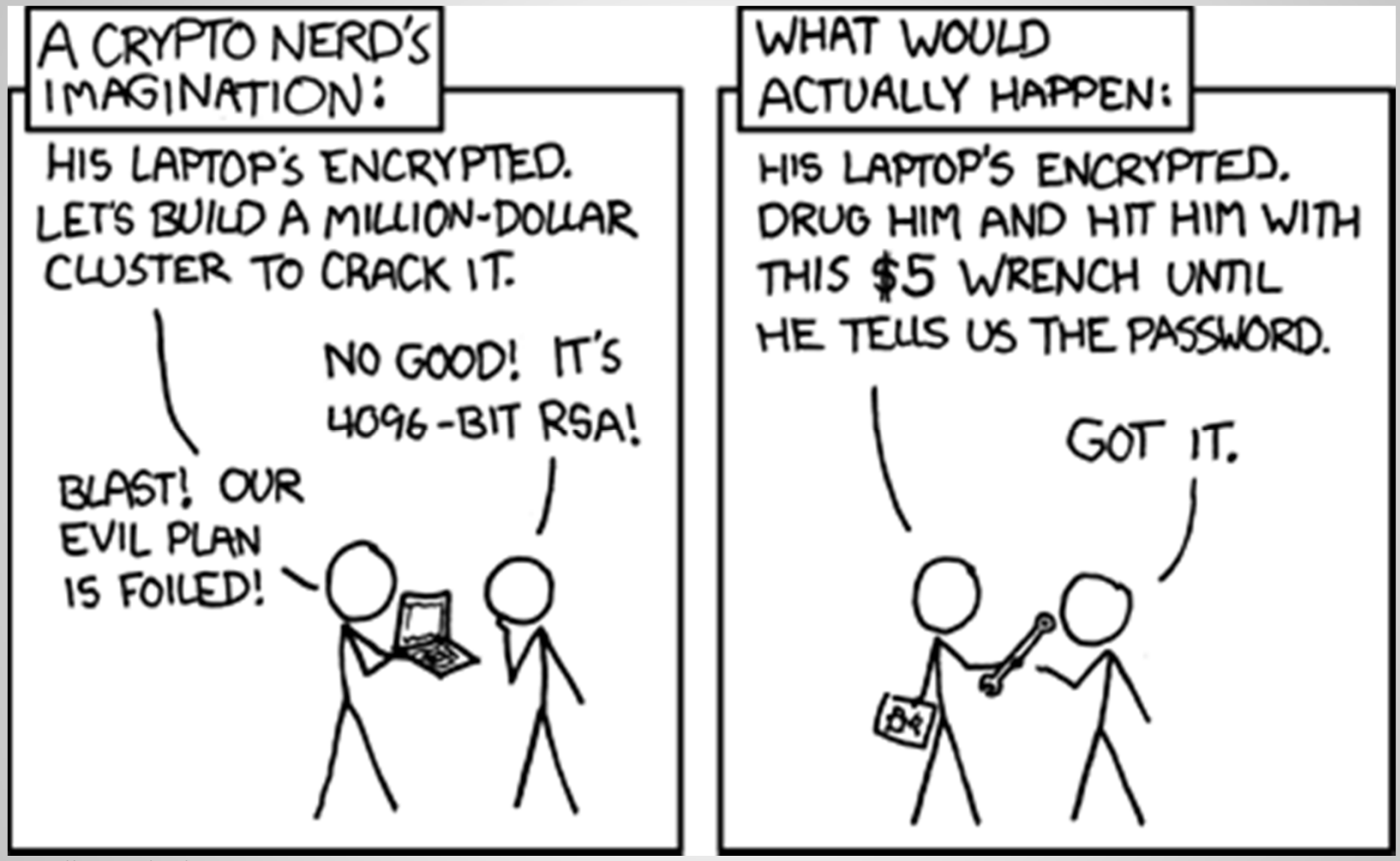
Is multilayer security good security?

- Increasing security burden
  - User-selected passwords to Kerberos passwords
  - Kerberos passwords to strong Kerberos passwords
  - 7 character to 14 character to ?
  - 2 factor: Strong Kerberos *plus* RSA token
  - 3 factor: Strong Kerberos *plus* RSA Token *plus* HSPD-12 badge
- Are we more secure?
  - Can we *PROVE* that we are more secure?

+

+

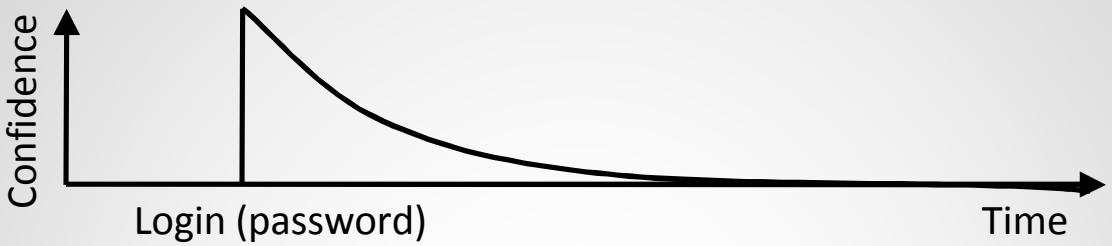
Rethinking our security approach.



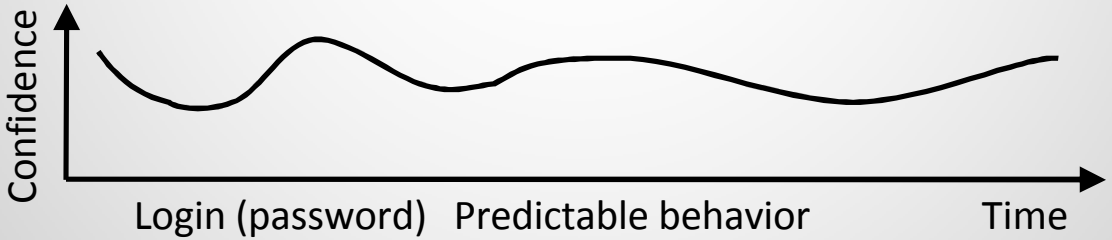
http://xkcd.com/538/

Continuous, adaptive identity authentication

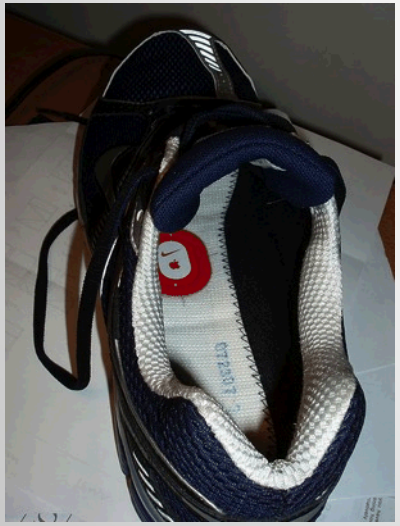
- **Event-based identity authentication** is momentary (event-based)



- **Continuous, adaptive identity authentication** is a continuous process
  - Probabilistic (not deterministic)
  - Approach: Multi-sensor fusion (example: Kalman filter using GPS, IMU, control laws, galvanic skin response, real-time DNA analysis, etc.)

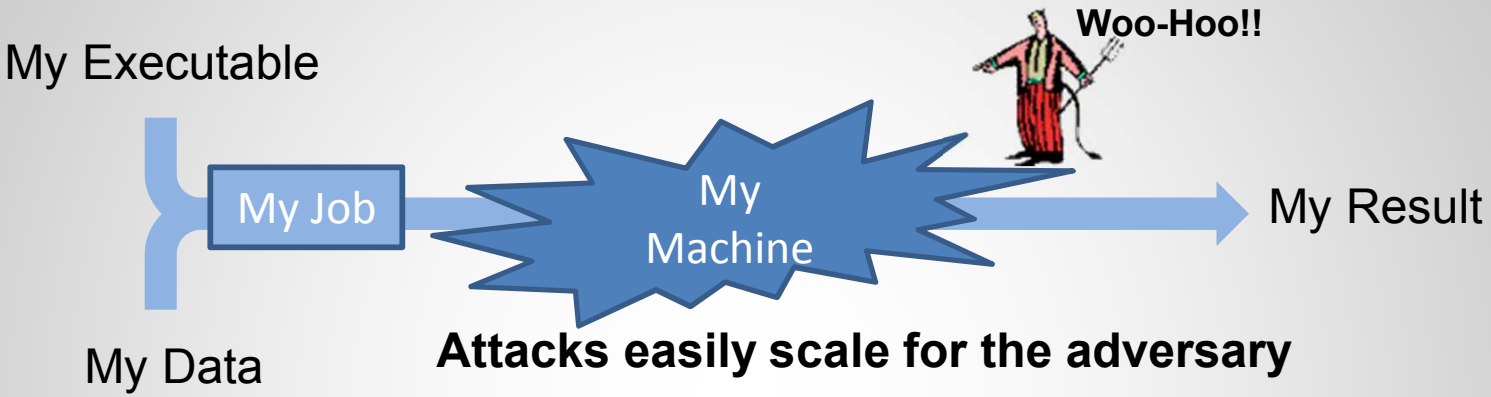


Continuous, Adaptive Authentication Approach



- INTEGRATION of existing sensors
  - ✓ Eyes
  - ✓ Gait (feet, waist)
  - ✓ GPS location
  - ✓ Voice
- to provide
  - ✓ Continuous
  - ✓ Real-time
  - ✓ Adaptive
  - ✓ Unambiguous
- identity authentication

Randomness does not exist today. We are all using the same executables

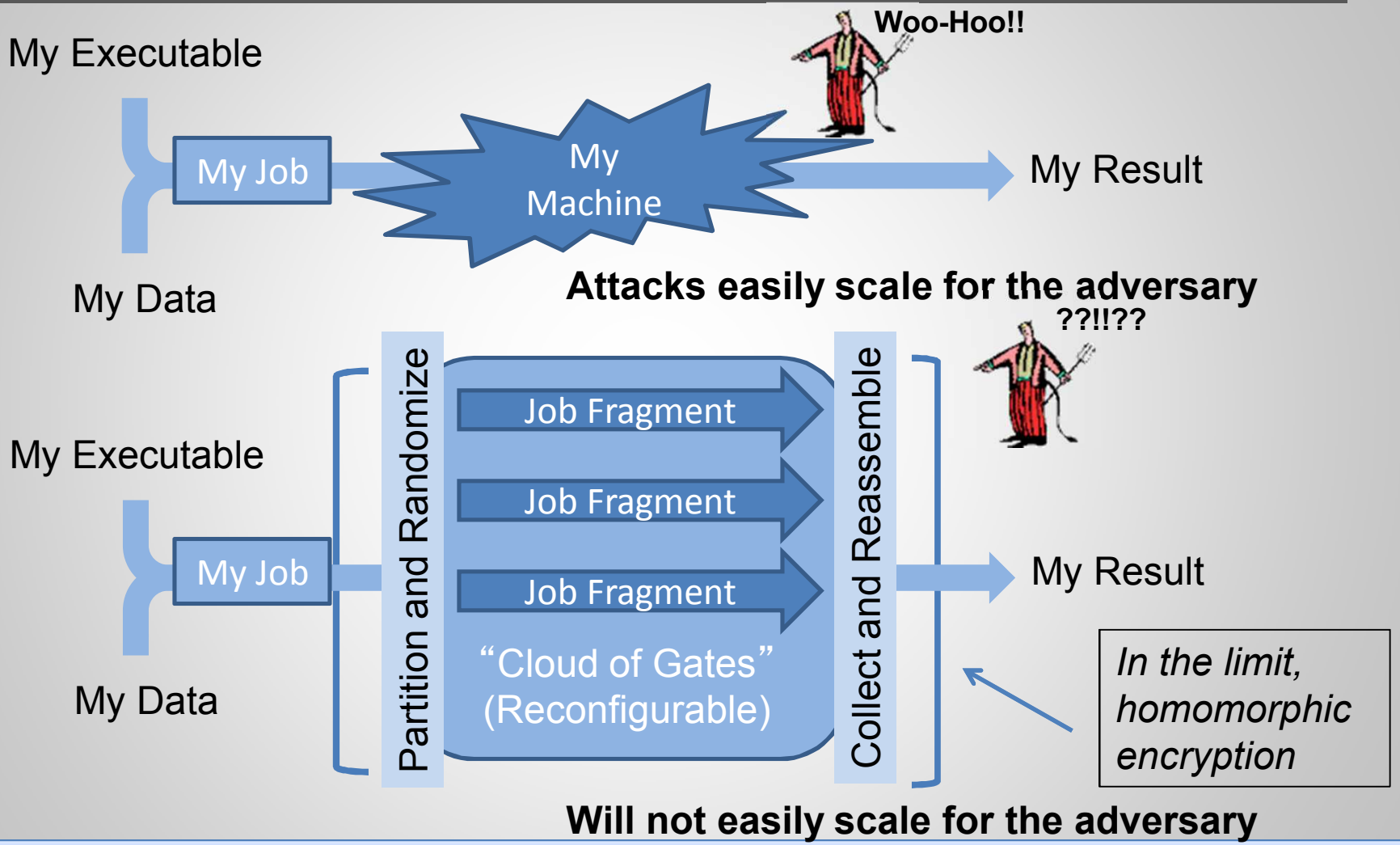


Reversing the asymmetry

- **The asymmetry**: the defender must protect against every possible exploit (hard) while the attacker need only find one unprotected vulnerability (easy) to achieve success.
  - A 25 year old bug in the BSD kernel was found a year ago.[1]
  - Microsoft identified security as job one for the Vista rewrite. After extended beta test, 6 major vulnerabilities were identified in the first 3 months after release.[2]
  - "Communities" of compromised machines on the Internet (i.e. Botnets) attack the cyber-infrastructure of Estonia (and now Georgia).[3]
  - Attackers find nooks and crannies in the combinatorial space (i.e. complexity) of our cyber-infrastructure to take control.
- **The approach**: Embrace cyber complexity and tailor it for the defense.

1. http://it.slashdot.org/story/08/05/11/1339228/the-25-year-old-bsd-bug
2. *blogs.technet.com/.../q108_2D00_client_2D00_scorecard.pdf*
3. http://news.cnet.com/2008-7349_3-6186751.html

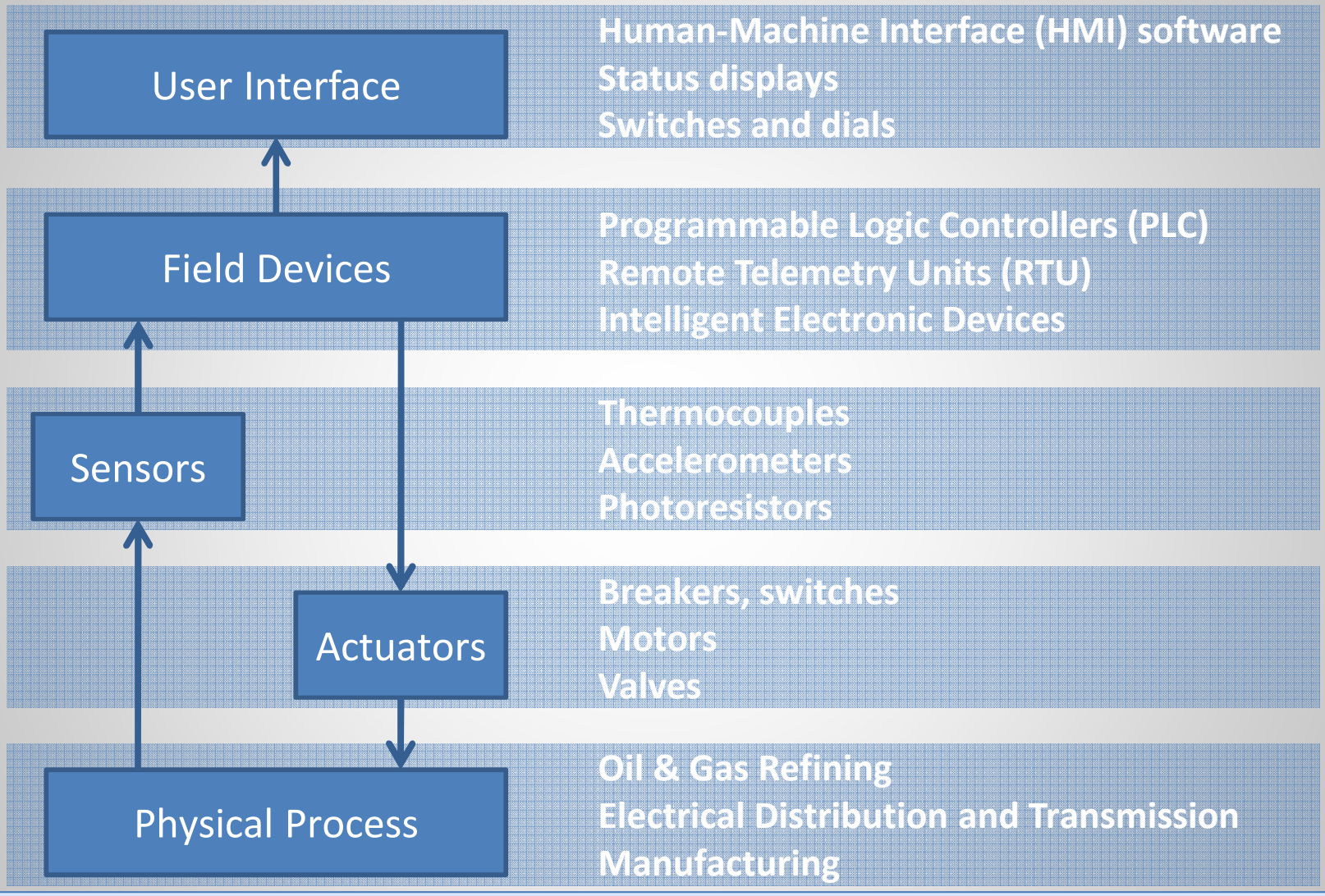
Reversing the asymmetry



WeaselBoard: A PLC Backplane Analysis System

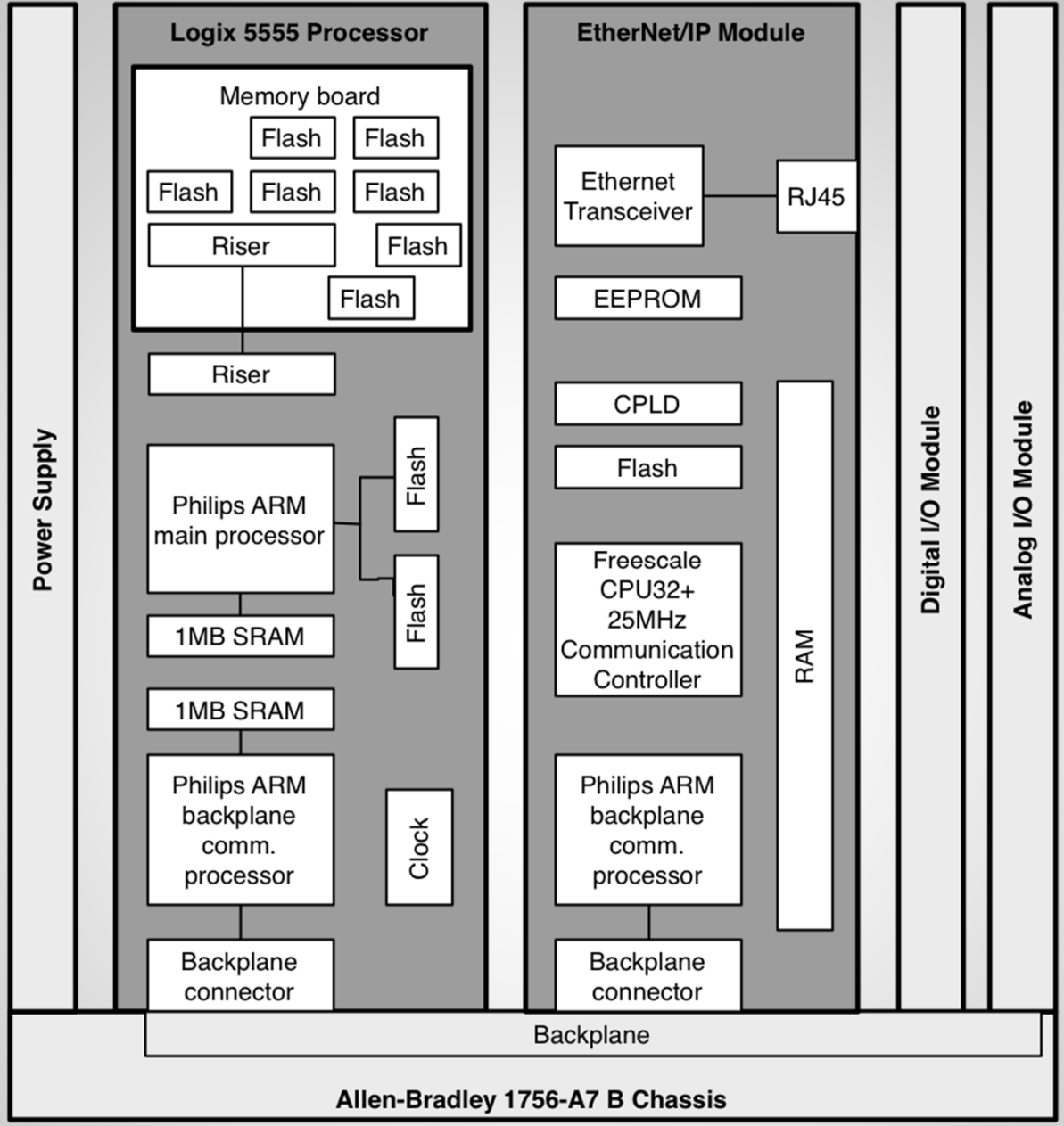
Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Control System Architecture



Allen Bradley Logix PLC

- Sold around 2005
- Processors: ARM or PowerPC
- OS: Wind River VxWorks


Power Supply
Logix 5555 Processor
Memory board
Flash
Flash
Flash
Flash
Flash
Riser
Flash
Flash
Riser
Philips ARM main processor
Flash
Flash
1MB SRAM
1MB SRAM
Philips ARM backplane comm. processor
Clock
Backplane connector
EtherNet/IP Module
Ethernet Transceiver
RJ45
EEPROM
CPLD
Flash
Freescale CPU32+ 25MHz Communication Controller
RAM
Philips ARM backplane comm. processor
Backplane connector
Digital I/O Module
Analog I/O Module
Backplane
Allen-Bradley 1756-A7 B Chassis

Problem

- United States critical infrastructures rely on Programmable Logic Controllers (PLCs) and similar component field devices for many key functions.
- Assessments have made clear that the control systems controlling our national infrastructure deserve more active cyber defense.

Need

- PLCs are vulnerable to targeted attacks that cost millions in equipment damage, lost operation, or injured personnel.
- PLCs are not monitored for security compromise.
- It is not enough to build “secure” products. The ability to inspect and detect is necessary for systems that will be in place for decades.

Solution: Independent Monitoring Device

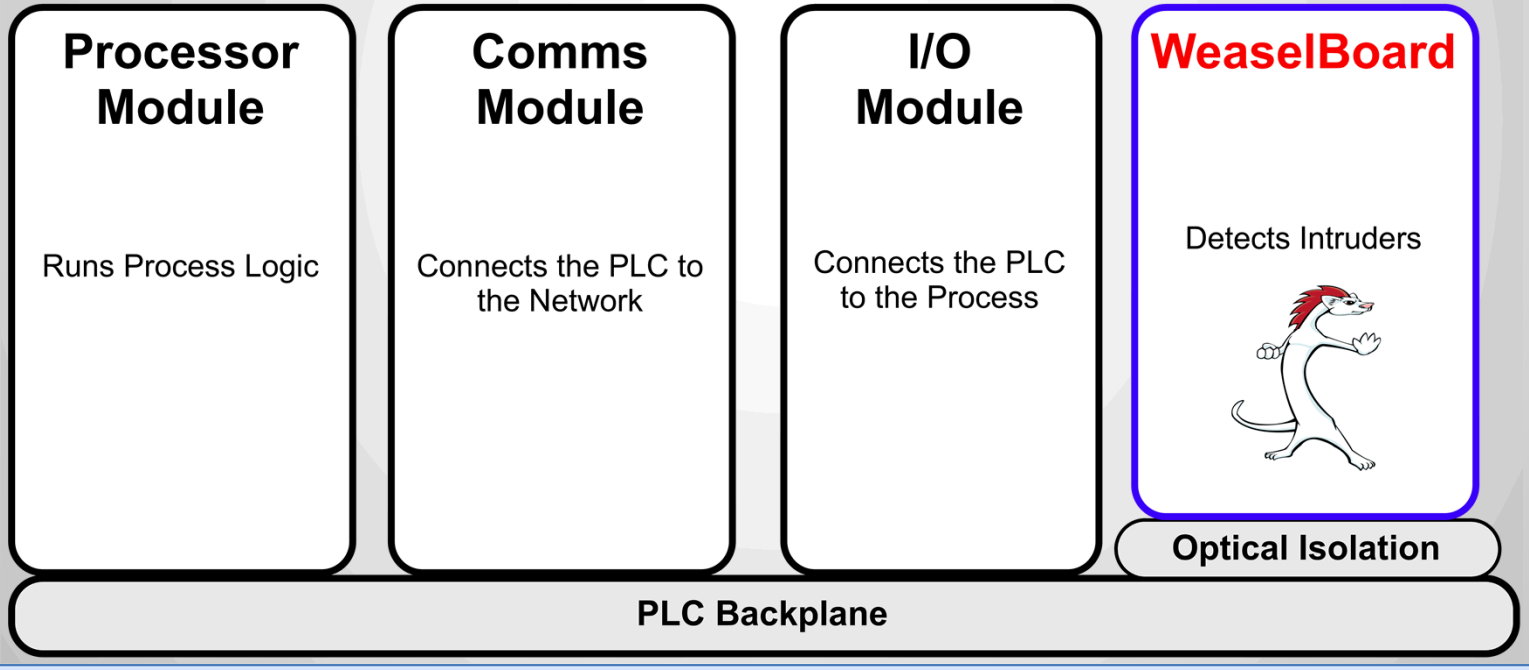
- A key element of the IMD concept is that the monitoring device's operation is independent from the system being monitored
- If the IMD operates independently of the system that it monitors, then subversions of the system will not be subversions of the IMD
- From this independent position, the IMD can act as a trusted observer in an otherwise untrusted system

Solution: Backplane Analysis System

- A backplane analysis system examines the communication between PLC modules
- Cyber attacks on the control systems will result in anomalies visible on the PLC backplane
- New Capabilities for PLCs:
  - Forensics: After compromises, detect modifications to hardware, firmware, or logic
  - Detection: Actively detect anomalies

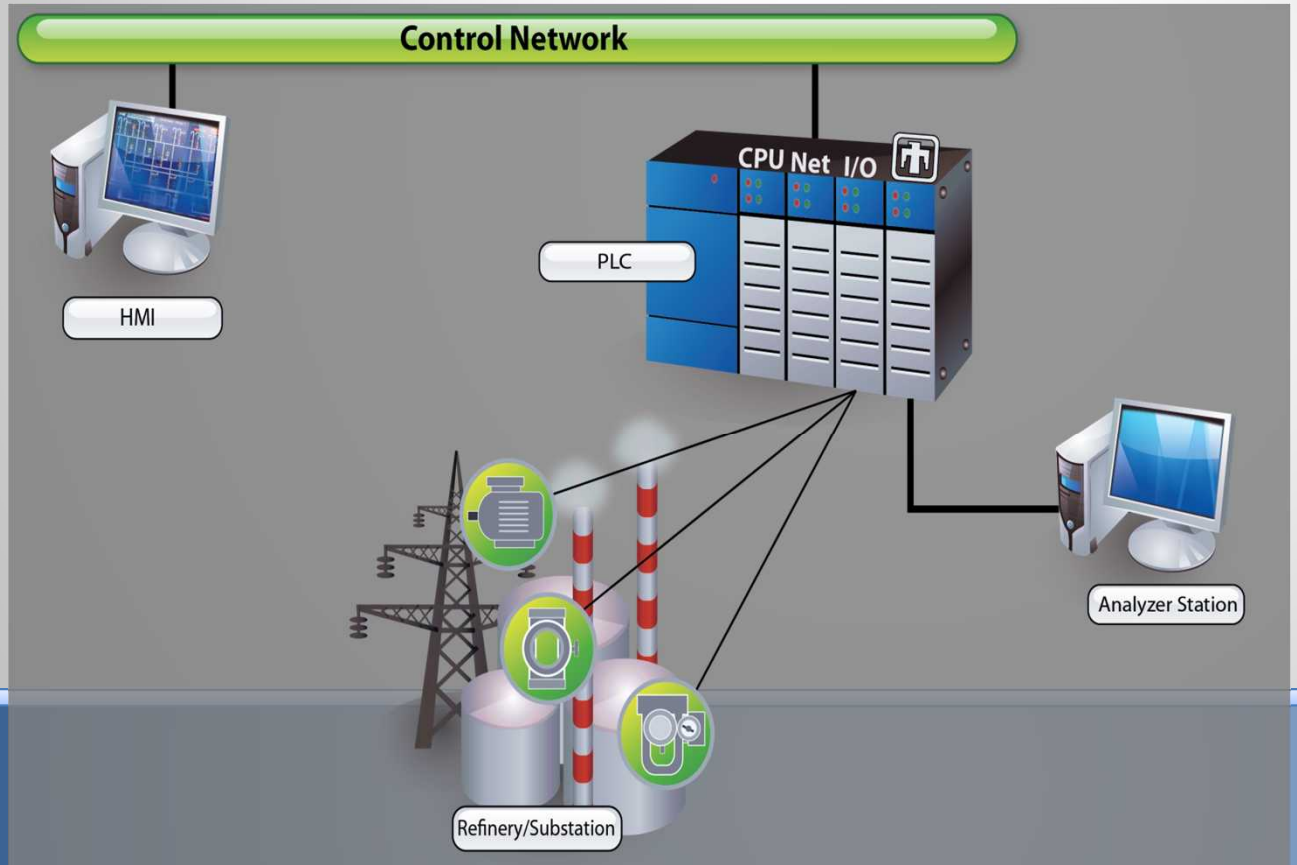
Approach

- WeaselBoard connects to PLC backplanes to capture traffic between modules.
- Alerts operators to malicious PLC behavior



Concept of Operations

- Detects any compromise that effect the process.
- Regardless of the source and location of the attack, WeaselBoard notices the attack's effect.



Things WeaselBoard Can Spot

- process control settings
- sensor values
- module configuration information
- firmware updates
- process control program updates

Outline

- National Laboratories Overview
- Who is Sandia National Laboratories
- Background on the evolving cyber threat
- A few cyber technologies we are likely to see in the next 5-10 years
- Opportunities:
  - Technical Internships to Advance National Security (TITANS)
  - Critical Skills Master's Program (CSMP)

TITANS (titans.sandia.gov)

- Technical Internships to Advance National Security (TITANS) offers stimulating internship experience in one of three technical tracks:
  - Center for Analysis Systems and Applications (CASA) – Develop next-generation software systems to solve the most complex and challenging data analysis problems our nation faces.
  - Center for Cyber Defenders (CCD) – Learn to combat cyberattacks, while gaining practical experience in understanding computer systems and network operations.
  - Monitoring Systems and Technology Intern Center (MSTIC) – Develop remote sensing and technologies for the next generation of national security systems.

CSMP

http://www.sandia.gov/careers/special_programs/critical_skills_program.html

- The Critical Skills Master's Program (CSMP) provides exceptional bachelor's-level candidates with the opportunity to receive fully funded master's of science degrees. Successful applicants will become regular full-time Sandia employees and will join multidisciplinary R&D teams that are advancing the frontiers of science and technology to solve the world's greatest challenges.