# Cybersecurity Operations in a Multi-Institutional Academic Setting: The NEES Story

**Saurabh Bagchi,** Fahad Ali Arshad, Gaspar Modelo-Howard
Network for Earthquake Engineering and Simulation (NEES)
School of Electrical and Computer Engineering
Purdue University

Joint work with: Brian Rohler, Thomas Hacker, Rudolf Eigenmann



Work Supported By: NSF, NEHRP



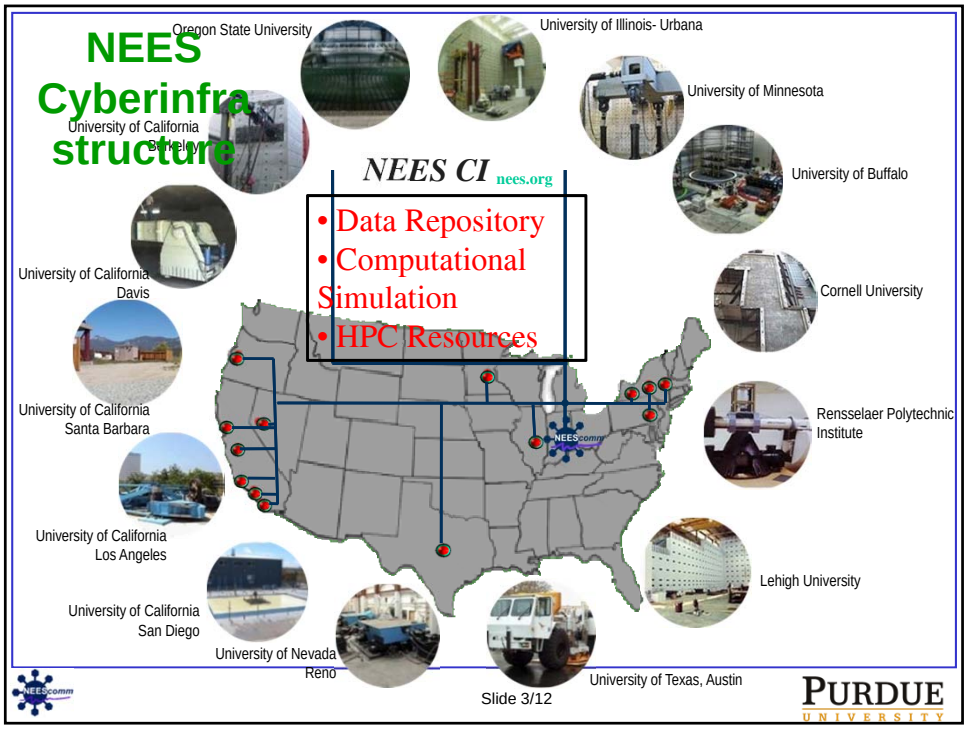
PURDUE UNIVERSITY

## What is NEES?

- Earthquakes and tsunamis can be devastating natural events
- To reduce the impact of these events, the George E. Brown, Jr. Network for Earthquake Engineering Simulation (NEES) originated in 2004 as a national, multi-user, research infrastructure
  - To enable research and innovation in earthquake and tsunami loss reduction
  - Create an educated workforce in hazard mitigation, and
  - Conduct broader outreach and lifelong learning activities
- Purdue took over in 2009 as the manager of a network of 14 advanced laboratories connected by a cyberinfrastructure
  - Anticipated end of that cooperative agreement is May 2015
  - The expectation of a future solicitation to continue the work



PURDUE UNIVERSITY



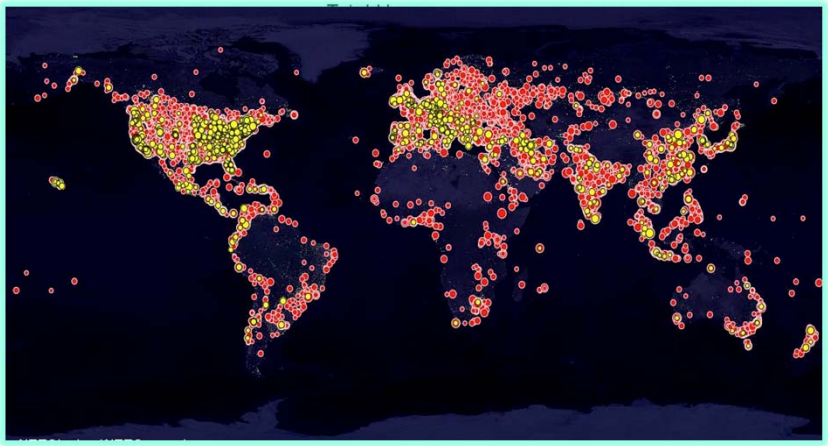



## NEEShub: Platform for Cyberinfrastructure

- The collaboration platform of NEES researchers, built on Purdue's HUBzero platform
- Links the NEES experimental facilities to each other, to NEEScomm, and to off-site users
- NEEShub has enabled researchers participating on-site or remotely to
  - Collect, view, process, and store data from NEES experiments
  - Central repository called Project Warehouse to store the curated data
  - Conduct numerical simulation studies, and
  - Perform hybrid (combined experimental and numerical) testing involving one or more NEES equipment sites

## NEEShub by Numbers

- NEEShub used by 78,177 distinct users in 2013
- Growing use from 212 countries since 2010





PURDUE UNIVERSITY

## Role of Cybersecurity in NEES

- NEES has developed a comprehensive cybersecurity approach that includes
  - Best practice cybersecurity policies and mechanisms at Purdue
  - An annual security audit and continual low-intensity scans at each of the NEES sites
- Goal: Walk the delicate line between
  - Prompt science and open community, AND
  - Preserving integrity and availability of our compute and data
- Personnel for cybersecurity
  - Me (faculty member in ECE/CS): 10% of my time
  - Cybersecurity staff engineer: 1.0 FTE (Gaspar)
  - Graduate research assistant: 0.5 FTE (Fahad)



PURDUE UNIVERSITY

## Result

- The result of a well-documented planning process and then the implementation and deployment has been
  - No reportable cybersecurity incident in the 5 years of existence
  - No major complaint from any of the stakeholders



## Unique Challenges for NEES Cybersecurity

1. Different universities have different cybersecurity policies and our policies had to “play nice” with them

2. We were responsible for doing security audits of equipment which we did not own or have root access on

3. How to test for external threats as well as internal threats? Notion of perimeter security is ingrained in technology and admins.

## How We Solved These Challenges

1. Varied cybersecurity policies
   - We sometimes enforced stronger rules for machines that are part of the NEES network
   - "Inner shell" of machines and other equipment (routers, PLC controllers, etc.) were created within the university IT resources
2. No ownership or root access on some equipment
   - Negotiated elevated privileges for purpose of security scanning
   - Success of human relation building: Feeling of being part of the same team
3. Test for external and internal threats
   - VPN access to sites for mimicking internal attacks
   - More stringent security controls at Purdue HQ



PURDUE UNIVERSITY

## The Twain between Cybersecurity Research & Practice

- As cybersecurity researchers, we have often bemoaned the slow adoption of our best research technologies
- Some successful topics where academic research has resulted in usable tools for security practitioners
  - Network/host intrusion detection: Bro, Tripwire
  - Vulnerability scanner: Nessus/OpenVAS, ZAP
  - Web server vulnerability assessment: Nikto
  - Static code analysis: Coverity
  - Blocking connections: fail2ban
- Areas where top quality research has not resulted in useful tools
  - Security configuration management: Example, for firewalls, SIM
  - False positives with signature-based systems



PURDUE UNIVERSITY

## Take Aways

- NEES at Purdue has operated an infrastructure at HQ and 14 sites for 5 years
  - With no reportable cybersecurity incidents
  - No howl of protest from the earthquake engineers and scientists
- Somewhat unique challenges that we faced, and partially solved are:

1. Different cybersecurity policies at the participating institutions
2. Responsible for security of IT assets that we do not control
3. Testing for external and internal threats

- Big gap between cybersecurity research and practice
  - A concerted attempt to bridge the gap will make life much easier



PURDUE UNIVERSITY

**Presentation available at:**
**Dependable Computing Systems Lab (DCSL) web site**
**engineering.purdue.edu/dcsl**

**Survey for collecting anonymous cybersecurity outage data:**
**At your cyberinfrastructure**
**https://purdue.qualtrics.com/SE/?SID=SV_4PBqU2cbN1yKTZP**



PURDUE UNIVERSITY