To submit questions, ask them in the discussion board on the virtual hub page.



# Targeted Formal Methods

Dr. Greg Shannon

Chief Science Officer

gregory.Shannon@cymanii.org

www.linkedin.com/in/gregshannon

This material is based upon work supported by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under the Advanced Manufacturing Office Award Number DE-EE0009046. The views expressed herein do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

# ~50 Minutes on These Topics, ~10 Minutes for Chat Discussion

- CyManII
- Perspectives on Progress
- Targeted Formal Methods
- Challenges and Opportunities

**I'll ask occasional questions.  #0 Do you remember your first hard proof?**

# The Cybersecurity Manufacturing Innovation Institute

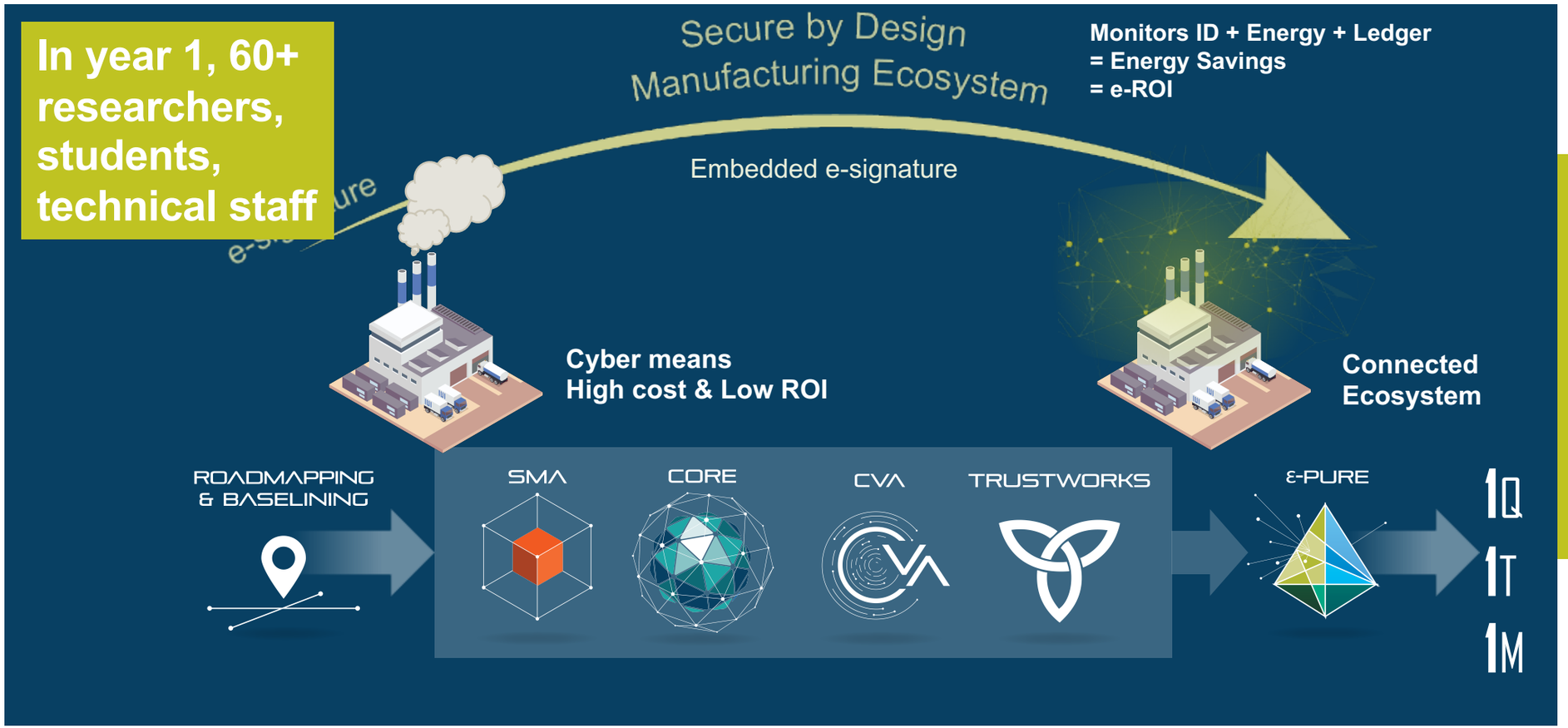
- March 2019, DOE asked for, *a Clean Energy Manufacturing Innovation Institute dedicated to advancing cybersecurity in energy efficient manufacturing*
- CyManII, is led by The University of Texas at San Antonio.
- The CyManII team of 59 members today is comprised of:
  - 3 Department of Energy National Laboratories (INL, ORNL, Sandia)
  - 4 other Manufacturing Innovation Institutes
  - 24 universities
  - 18 companies
  - 10 nonprofits

Gabriela Ciocarlie
Dongyan Xu
David Nicol
Bill Harrison

**CyManII's public launch is Thursday, November 19th**

CYMANII

# A 5-Year $111M Department of Energy Investment




**Focus on 8 sectors:**

- Iron & Steel
- Petroleum Refining
- Semiconductors
- Clean Energy
- Food & Agriculture
- Cement
- Transportation Equipment

**Produces cybersecure energy-efficient innovations for secure and positive returns on investment**

# Key Practical Elements in CyManII's Technical Work

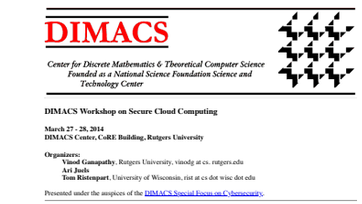
- From the start
  - Agile methods for research, development, engineering, and operations
  - Continuous Integration Continuous Delivery (CI/CD)
  - DevSecOps
- We anticipate adversary interest
  - Goal: an efficient and secure innovation pipeline / supply chain
- How we do our work affects the degree to which we successfully incorporate targeted formal methods (and vice versa)

# Audience Question #1

- Do you have methods or results that are ready to be applied to practical problems in digital and cyber-physical security?

# Perspectives on Progress from a Particular Perch

- 2014 DIMACS Workshop on Cloud Security
  - inherently_improved_security = hard_problems + automated_structured_reasoning
- 2015 IEEE Cybersecurity Initiative
  - Security tools and methods that engineers/developers can use
- 2016 Federal Cybersecurity R&D Strategic Plan
  - Defense-based deterrence requires experienced/demonstrated difficulty of success
- 2017 JASON Study on Industrial Scale Formal Methods (for security)
  - Industry is getting serious about using formal methods
- 2019 UTSA CyManII Proposal
  - Only formal methods are sufficiently efficient to make vulnerabilities hard to find
- 2020 AF-SAB Avoiding Unintended Behaviors in Autonomous Systems
  - Industry leaders are scaling up their use of formal methods; physics helps


DIMACS

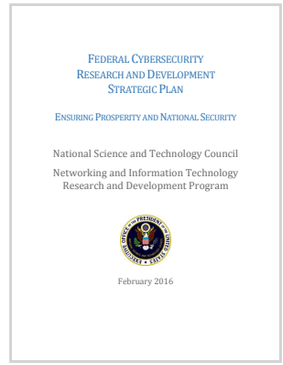
Center for Discrete Mathematics & Theoretical Computer Science
Founded as a National Science Foundation Science and Technology Center

DIMACS Workshop on Secure Cloud Computing

March 27 - 28, 2014
DIMACS Center, CoRE Building, Rutgers University

Organizers:
Vinod Ganapathy, Rutgers University, vinodg at cs. rutgers.edu
Ari Juels
Tom Ristenpart, University of Wisconsin, rist at cs dot wisc dot edu

Presented under the auspices of the DIMACS Special Focus on Cybersecurity.


FEDERAL CYBERSECURITY
RESEARCH AND DEVELOPMENT
STRATEGIC PLAN

ENSURING PROSPERITY AND NATIONAL SECURITY

National Science and Technology Council
Networking and Information Technology
Research and Development Program

February 2016


CYMANII

# Audience Question #2

- What new documentation for insights and evidence of value are you seeing in the actual application of formal methods?

# Consider

- If the model's wrong, what can we still learn running the proofs?
  - Counterexamples
  - Model errors
- If the proof doesn't complete, have we learned anything?
  - Knowing the "truth" is hard and finding counterexamples is not easy
- If the proof hasn't completed, why stop?
  - Our adversaries are always looking, why aren't we?

CYMANII

# What Do We Mean by Targeted Formal Methods?

- Adequate
  - Enough – no more than needed
  - Simple is great
- Agile
  - Incremental modeling
  - Incremental properties
- Consequential
  - Consequence/threat/risk avoidance
  - Elucidation of assumptions
  - Efficiency of analysis

- Example–CyManII access control
  - Can UTSA credentials (w/ Dou) access CyManII's wiki?
  - Can CyManII credentials (w/out Duo) access CyManII's wiki?
  - How do we validate our model and make it increasingly more realistic?
  - What is the "easiest" way to "break our proofs" and achieve access?
    And maybe discover an inadequate assumption?

# Audience Question #3

- What is your favorite example of a targeted application of formal methods?

# Opportunities to Solve Technical Challenges

| Challenges | Opportunities |
|---|---|
| Computational intractability / complexity | → Custom hardware inference accelerators: $10^6$x faster?<br>→ AI in the logic engines to exploit unknown or hard to characterize problem-instance structure: $10^3$x faster?<br>→ Develop a theory of the value in unfinished proof / counterexample searches: empirical lower bounds? |
| Small trained/trainable workforce | → Modern development tool chains for continuous integration and delivery<br>→ Proof engineering and engineers targeted and evolving use of particular methods and their tool-chain integration |
| Gaps between real entities (e.g., systems) and the models for which proofs are sought | → Agile development with continuously identifying gaps via<br>→ operational validation<br>Develop a theory of ”almost counterexamples” |

**Interesting opportunities for focused R&D investments**

CYMANII

# A Recurring Non-technical Challenge

- Formal Methods have a poor reputation for practical and scalable application on more than just a few special problems
  - Scarred (and scared?) in the Discrete Mathematics class?
- For critical systems, with an intelligent/adaptive adversary, what's the alternative to efficient careful thinking and automatable analysis?
  - Wetware and CNNs alone won't win (for us) ihmo

# Audience Question #4

- What Challenges and Opportunities do you see in creating practical value in applied formal methods?

# Questions?

This material is based upon work supported by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under the Advanced Manufacturing Office Award Number DE-EE0009046. The views expressed herein do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

To submit questions,
ask them in the discussion board
on the virtual hub page.

You can also use this area to continue the discussion after the presentation as speakers will be checking for new comments throughout the summit.