|galois|

Scaling
Formal Methods in the Field
at Galois

NSF Formal Methods in the Field PI Meeting 2024

November 12–13, 2024

Joe Kiniry

Galois

galois

Advancing computer science R&D
Creating trustworthiness in critical systems

Computer Security - Correctness - Cryptography
Cyber-Physical Systems - Data Science - Formal Methods
Human-Computer Interaction - Languages - Machine Learning
Rigorous Digital Engineering - Semiconductors

Clients

AWS
DARPA
DHS
DOD
DOE

IARPA
NASA
NIH
NIST

NRC
NSA
NSF
SDA

Offices

Portland, OR
Dayton, OH
Arlington, VA
Minneapolis, MN

History

Founded in 1999
120+ employees

Spin-outs

Tangram Flex
Niobium Microsystems
Free & Fair
ExistX
TOZ
Muse.dev

A different kind of company

No managers

We have no fixed hierarchy of rigid positions and titles, and no traditional managers.

Choose your work

Research engineers choose the projects they work on, and move freely between projects depending on personal interests and career goals.

Radical transparency

Everything is transparent by default: company financials, decision making, open meetings, and even salaries.

Ownership

Employees own the company together, making important decisions as a group and partaking in the financial success of the company.

More info at **lifeatgalois.com**

Thanks for the Invitation

- Our thanks Katherine, Garrett, and Cesare for thinking to invite us.
- We love to participate in these kinds of events, as R&D funded by NSF often is the shoulders on which we stand transitioning FM into industry.
- We also learn about new tools (those mentioned by Aaron), get updates on tools we have used a bit (e.g., Cedar and PVS), and hear from many Friendwegians (friends of Galois—we are Galwegians).
- This monotonically grows our toolbox of >100 formal methods, and increases our set of potential collaborators.

Galois: 25 Years of Formal Methods

- Galois turned 25 in October of this year.
- For years we had only one client that was focused on the development and use of Cryptol.
- Hard times in R&D funding in the 00s made us realize that we needed more than one client.
- We tried to spinout our first company (Signali Corp), but that was *very* badly timed (2009).
- I joined Galois in 2013—we had around 40 employees, one office, and a handful of clients.
- Today we have >100 employees, four offices, half a dozen daughter companies, are nearing 300 employees across all of them, and have to turn down work.

Our Strengths and Limitations

- Galois employs many of the best formal methods researchers and engineers in the world.
- But virtually all of our work is “butts-in-seats” R&D.
  - basic and applied R&D for Government clients
  - Work-for-Hire development or assurance work for industry, esp. the DIB, Fortune 10, and “crypto”
- Circa 50 formal methods FTE a year spread across several dozens projects only goes so far.
- We must find ways to magnify our and *formal methods in the field* impact, with the resources (people and time) and clients we have today.

The Forcing Function for Change

- President Biden's National Cybersecurity Strategy
- Executive Order 14028 on Improving the Nation's Cybersecurity (2021)
- National Security Memorandum (NSM) 5, "Improving Cybersecurity for Critical Infrastructure Control Systems"
- NSM 8, "Improving the Cybersecurity of National Security, Department of Defense (DoD), and Intelligence Community Systems"
- NSM 10, "Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems"
- National Cybersecurity Strategy Implementation Plan, May 2024 Version 2

How did we help with, and how do we respond to, this change?

The Galois Strategy

spinouts

training

tools

IP

Spinouts

- Galois: trust your most critical systems
- Tangram Flex: rapid integration with confidence
- Niobium Microsystems: domain-specific ASICs
- Free & Fair: democracy as a critical system
- ExistX: “applied” Galois for classified systems
- TOZ: applied cryptography for all
- Muse.dev: integrating formal analysis into CI/CD

- And there is more to come in 2025 and beyond…

  Reach out to collaborate, tell us about your methods and tools, or to talk about a career.

Training

- *Cryptol* and *SAW* are the de facto standard tools used for Government formal specification and verification of cryptographic algorithms.
    - Cryptol and SAW courses are regularly given to Government, DIB, and corporate teams.
- *Rigorous Digital Engineering* (RDE) is being adopted by several Government and DIB teams as the practical way to bring formal methods into the field.
    - DARPA funded the development of an RDE course that is now being given to Gov and industry.
- Our aim is to “train the trainers” so that the training materials can be reused without us.

Tools

- Formal methods will only have a broad impact if everyday engineers can actually *use* tools.
- What do clients really care about historically?
  - Cheaper >> Faster >> Better
  - Faster >> Low Energy >> Secure
- Tools *must* have commercial support, but also *cannot be expensive*, *lock in customers*, or *demand high NRE costs*, such as high training time/costs or enormous changes to corporate process/methods.
- Clients love a tool or technology that is open source (cheap!), but also are frightened by that transparency and do not understand rigorous evidence.

Intellectual Property (IP)

- Our last way to put formal methods in the field is through the creation of reusable, maintainable, extensible IP that is licensed to clients.
- Open Source libraries/frameworks/modules is one kind of non-tool IP that is licensed for use.
- Proprietary tools and software, firmware, and hardware IP components is another fruitful path.
- Companies licensing IP developed with formal methods is often changes their expectations for existing suppliers.
    - IP comes with literate documentation, formal specifications, out-of-the-box evidence of testing- and formal verification-based correctness and security, and rich demonstrations of use

The Upside Down of Formal Methods

- Today, many upcoming RFPs will regularly mention *formal methods and generative artificial intelligence.*
- Government procurement and certification are evolving to demand *specifications and evidence.*
- Recommendations about safe languages, security-centric hardware architectures, and applied formal methods are becoming *standard best practices.*
- There will be a *tremendous growth in hiring and retraining* for software, hardware, and systems engineers willing to learn and use more modern languages, tools, and technologies that leverage formal methods explicitly, or in *secret ninja ways.*

Wrapping Up

- The world needs more people to be able to “do” formal methods, in the real world, on real systems.
- We need more software, firmware, and hardware engineers to use formal methods, whether they know it or not.
- There is a sea change going on in Five Eyes countries.
- These changes are impacting our day-to-day R&D, and may influence future NSF focus. *Pay attention young academics.*
  - safe languages are the future,
  - secure hardware is critical, and
  - and formal methods are very important.
- => Galois is hiring, and clearance is now necessary.
- => Galois is constantly collaborating with academic institutions and other companies that complement us.