



Applying Formal Verification to Make a Difference

Jim Grundy (he/him)

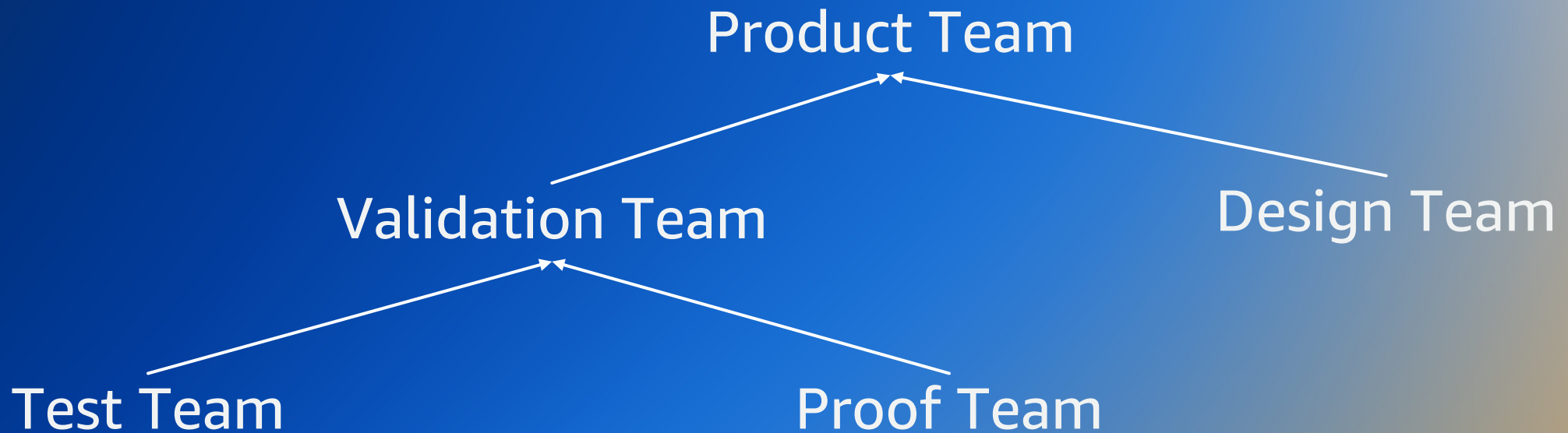
jmgruj@amazon.com

Who should you hire?

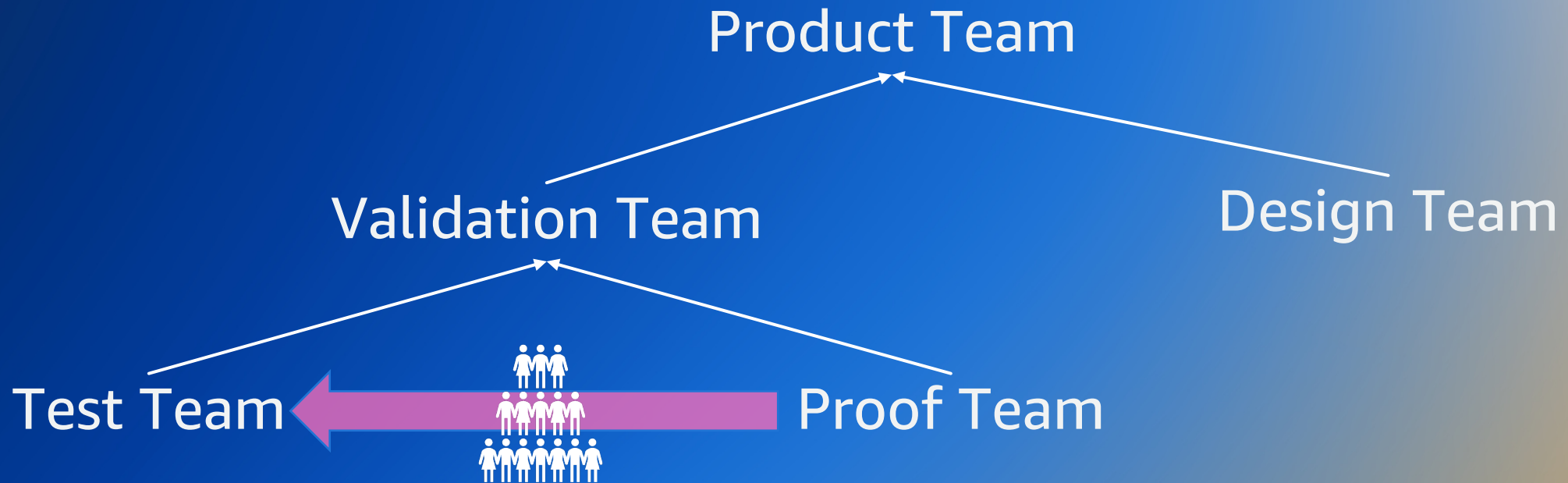


What should the project organization look like

You want to avoid this structure



Because this will happen



This structure can help for a while



The goals you take predict success



A (glorious) failure



Containing a kernel of success



Solving entire problems is a good goal



How to sell new proofs



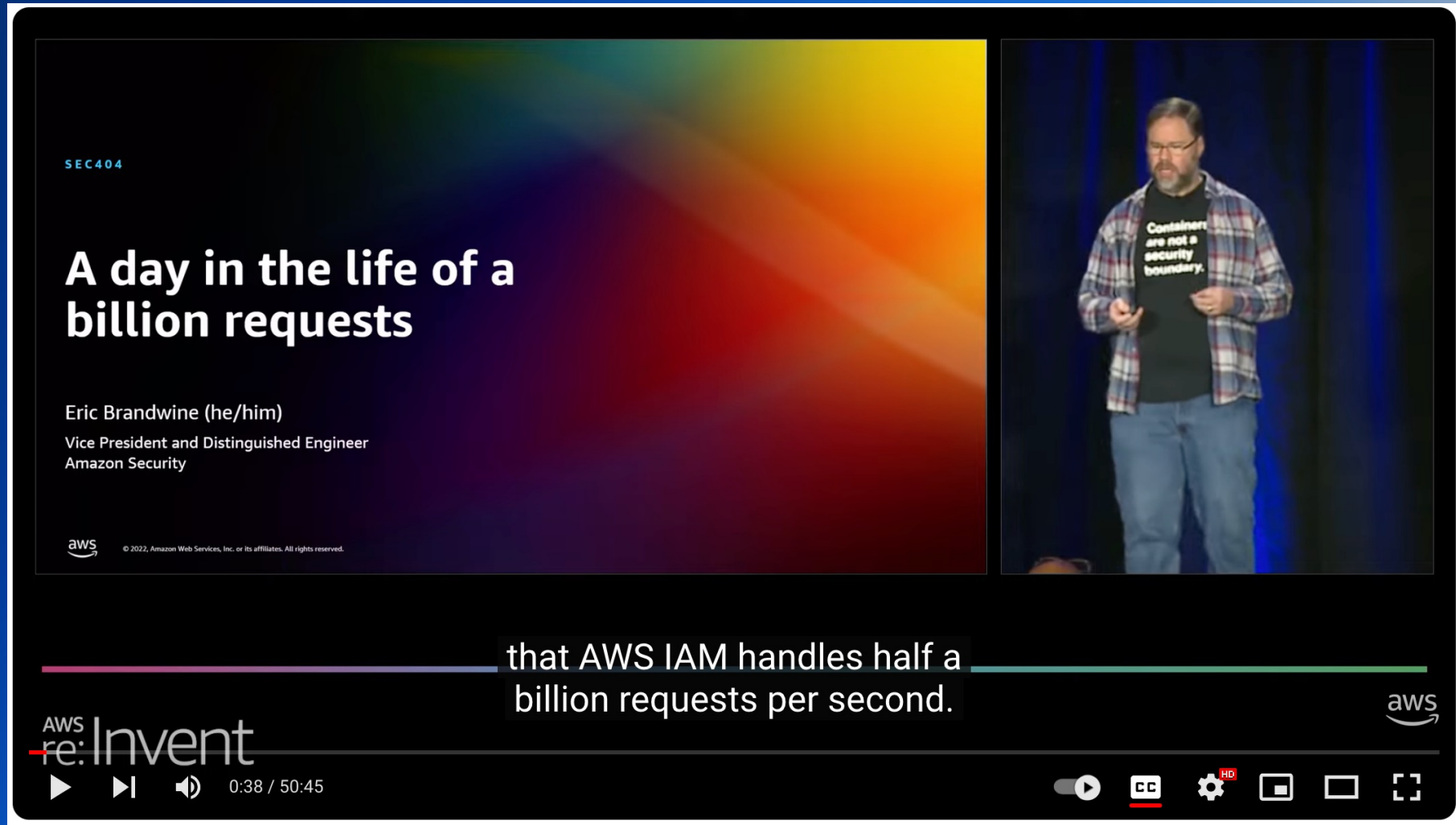
Selling software FV to a hardware company



Why care about software?



Formally Verifying Public Key Crypto



The screenshot shows a video player interface. On the left, a presentation slide is displayed with the following text:

SEC404

A day in the life of a billion requests

Eric Brandwine (he/him)
Vice President and Distinguished Engineer
Amazon Security

aws © 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

On the right, a speaker is shown on stage wearing a plaid shirt and a black t-shirt that says "Containers are not a security boundary."

Below the slide, a subtitle reads: "that AWS IAM handles half a billion requests per second."

The video player controls at the bottom include the AWS re:Invent logo, a play button, a progress bar at 0:38 / 50:45, a volume icon, a CC icon, a settings gear, an HD icon, a full screen icon, and a share icon.

Proving RSA for Graviton2

AWS Graviton Processors

Get the best price performance for cloud workloads running on Amazon EC2

Get Started with Graviton-based EC2 Instances

Quickly innovate with AWS Graviton Fast Start

Try Amazon EC2 t4g.small instances powered by AWS Graviton2 processors [free for up to 750 hours per month](#) until Dec 31, 2023.



Recap



Quick tour of ITP at AWS



Project X



s2n-bignum

The screenshot shows the GitHub repository page for `aws-labs/s2n-bignum`. The repository is currently on the `main` branch. The `README.md` file is selected, showing a merge commit by `jargh` titled "Merge branch 'aws-labs:main' into main" with commit hash `a300a7f` from last year. The file size is 477 lines (384 loc) and 22.2 KB. The README content is as follows:

s2n-bignum [↗](#)

This is a collection of bignum arithmetic routines designed for cryptographic applications. All routines are written in pure machine code, designed to be callable from C and other high-level languages, with separate but API-compatible versions of each function for 64-bit x86 (`x86_64`) and ARM (`aarch64`). Each function is written in a constant-time style to avoid timing side-channels, and is accompanied by a machine-checked formal proof that its mathematical result is correct, based on a formal model of the underlying machine.

Semi-automated block ciphers and hashes

☰ README.md

AWS libcrypto (AWS-LC) [↗](#)

AWS-LC is a general-purpose cryptographic library maintained by the AWS Cryptography team for AWS and their customers. It is based on code from the Google BoringSSL project and the OpenSSL project.

AWS-LC contains portable C implementations of algorithms needed for TLS and common applications. For performance critical algorithms, optimized assembly versions are included for x86 and ARM.

Cedar DSL for authorization

Cedar: a new language for expressive, fast, safe, and analyzable authorization



Emina Torlak

Sr Principal Applied Scientist, AWS
Affiliate Professor at the University of Washington

Joint work with

Craig Disselkoen, Aaron Eline, Shaobo He, Mike Hicks, Kesha Hietala, John Kastner, Anwar Mamat, Darin McAdams, Neha Rungta, and Andrew Wells (all at AWS), and many others



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Thank you!