OpenSSL CONFERENCE

The Last Mile of Trust

4,500,000 patient records

Compromised third-party VPN appliance

2014

Heartbleed

TIME: FRIZELL, SAM. "REPORT: DEVASTATING HEARTBLEED FLAW WAS USED IN HOSPITAL HACK." TIME, AUGUST 20, 2014.

OpenSSL CONFERENCE

Math vs. Implementation

- Missing length validation on a RFC 6520 heartbeat request →
- Adjacent memory disclosure

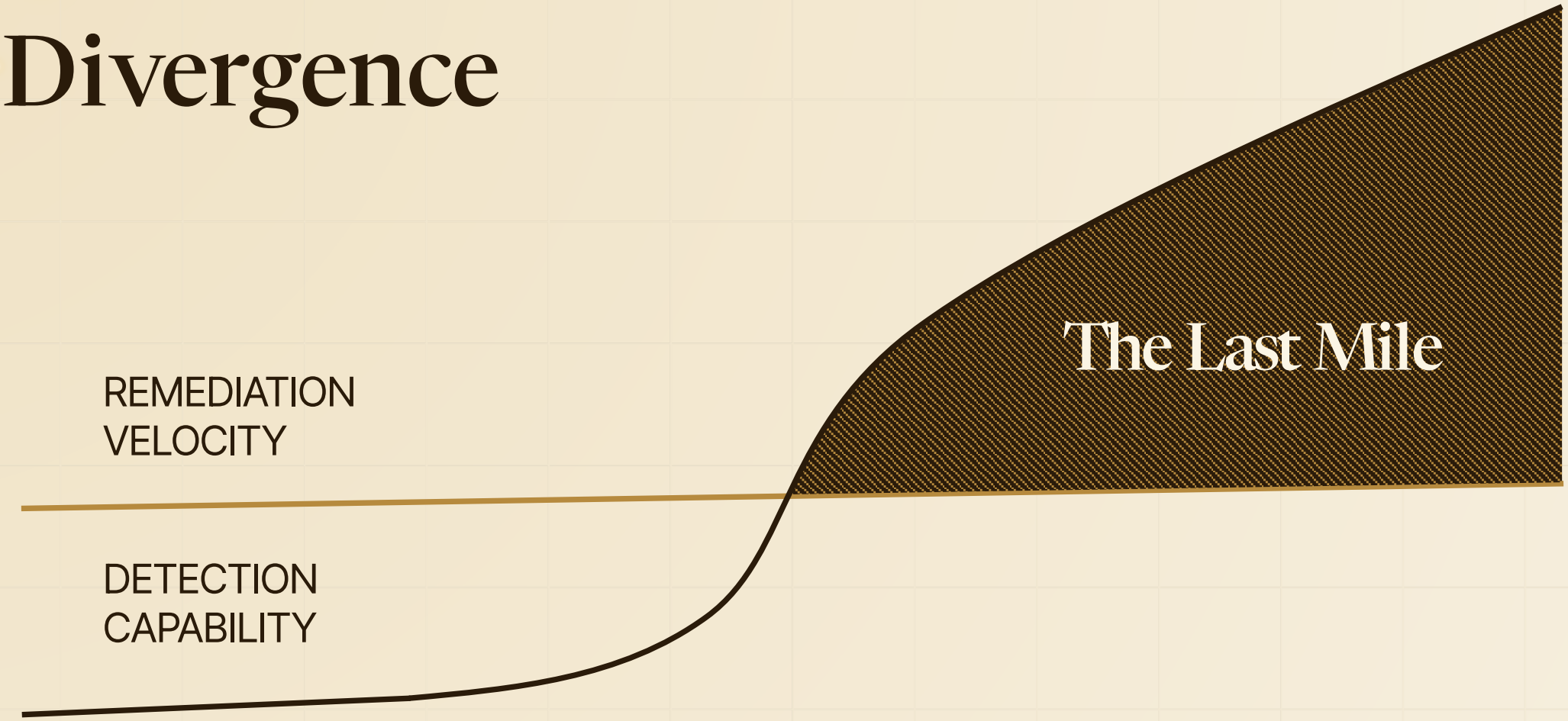
~2 years
in public code before disclosure

12 years
since disclosure

34,000
devices still exposed a decade later*

* EDGESCAN VULNERABILITY INTELLIGENCE: 2024 EDGESCAN VULNERABILITY STATS REPORT

Divergence



Securing the last mile is a shared problem

10s of millions of devices

5+ year lifecycles
many past end-of-support, still running

* REPORTED BY CISA, EDGESCAN (2024), AND LANSWEEPER (2025).

Fix Available

(Day 0)

~80% of organizations operate in this gap

Fix Deployed

(6+ Months)

OpenSSL CONFERENCE

// TIME_ELAPSED

14 WEEKS

Analysis timeframe

// CODEBASE_VOLUME

6.78B SLOC

Source lines of code analyzed

// LANGUAGE_PARSERS

28 LANGUAGES

Polyglot AST support

// DYNAMIC_VERIFICATION

Pass LIVE_EVAL

Exploits validated in live sandboxes

≈12.0 Full Time Engineer Years

(Cumulative Security Research Output)

The industry pivot to hardening releases

// OLD_MODEL

Individual vulnerability fixes shipped per advisory

// NEW_MODEL

Batched hardening releases

The Real Constraint:

Customers cannot consume individual vulnerability fixes at the rate AI finds defects

Why we standardized on OpenSSL

/01/

Transparency

/02/

Quality through scrutiny

/03/

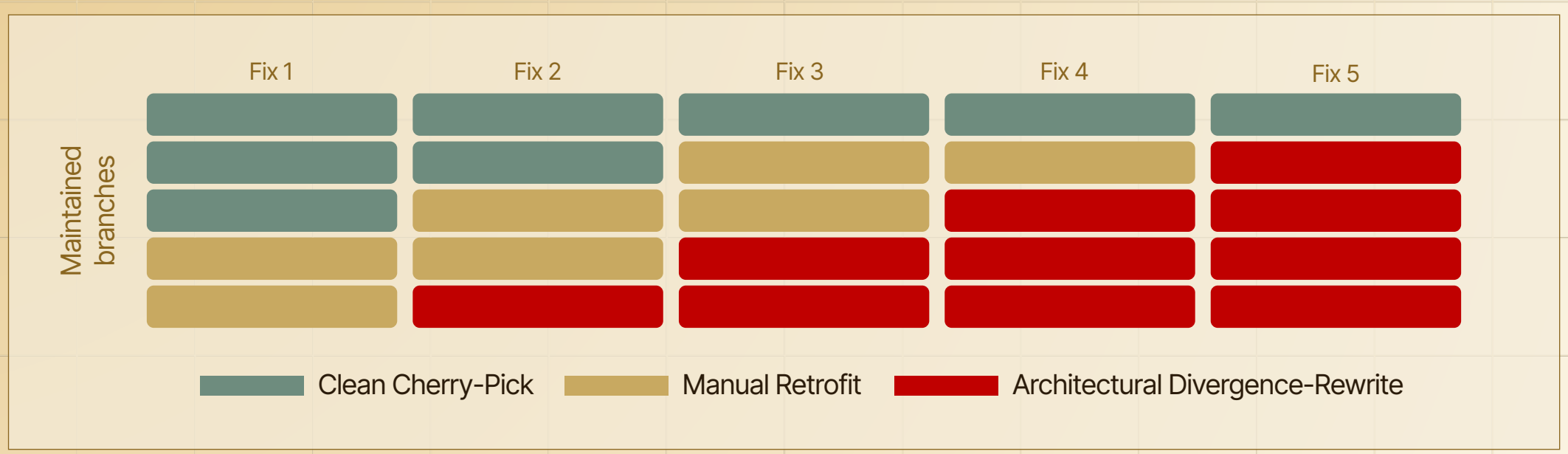
Trust with global customers

Why we forked

- FIPS 140-3 validation boundaries and timelines
- Customer security standards
- Feature gaps
- Release cadence mismatch

It worked. For us.

The Compounding Cost



Cascade: The Inevitable Multiplier

BRANCH TAX → FEATURE TAX → LOST SCRUTINY → SLOWER PROPAGATION → SLOWEST LAST MILE

Volume of AI-discovered findings

(100s–1000s per module)

Time-from-disclosure-to-exploitation, trending toward zero

Convergence Point

Agentic AI, both directions

Field exploitation rate, rising

OpenSSL CONFERENCE

Post-Quantum Cryptography

/01/ Not Drop-In

/02/ Protocol Modifications

/03/ Performance

/04/ Resource Constraints

/05/ Hybrid vs. Pure

/06/ Geopolitical Fragmentation

/07/ AI-driven Iteration

OpenSSL CONFERENCE

A Different Approach

Premium Patron of the Open SSL Foundation

Funding + Direct Engineering Resources

Ryan Hooper

Working Directly for OpenSSL

Jeff Johnson

Elected, OpenSSL Corporation
Business Advisory Committee

Barry Fussell

Elected, OpenSSL Foundation
Technical Advisory Committee

Concrete Outcomes

Accelerated DTLS 1.3 (RFC 9147) delivery, enabling Post-Quantum Cryptography in datagram protocols /01/

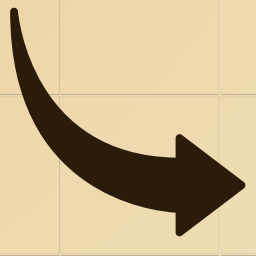
Expanded capacity to triage the incoming volume of AI-discovered findings /02/

Feedback loop that materially reduces the need to fork /03/

What we can do

Individual Contributors	Start: pick something easy from the back-log, and work on it
Academia	Billy Brumley needs your help – we need more of you
Small Business	Leadership in business advisory committees needed
Operating System (OS) Distribution	Thank you for all your support – keep up the good work
Enterprise/Large Business	Attend monthly business community meetings; share perspectives, solve common issues, define roadmaps
Foundation/Peers	Funded seats, non-profit donations

What we can do



https://openssl-communities.org/hub

The math was never the hard part

Security is a team sport –
the last mile is our shared responsibility