ISRG Internet Security Research Group

Building a better Internet

2023 ANNUAL REPORT

https://abetterinternet.org

Our first decade

INTERNET SECURITY RESEARCH GROUP

Ten years ago, ISRG was founded to tackle what at the time seemed like an insurmountable challenge: encrypting the Internet. As a nonprofit ISRG has proliferated free TLS certificates to billions of websites via Let's Encrypt, creating an Internet that is more secure and privacy respecting.

Today ISRG remains focused on ensuring the Internet is secure beyond just encryption. Through its projects, ISRG is bringing memory safety to critical software behind the Internet, including the Linux kernel, and standardizing a new paradigm for privacy-respecting data analysis.

Contents

Our tenth anniversary

TEN YEARS OF BUILDING A BETTER INTERNET

In 2013, the idea of building a new certificate authority (CA) was not necessarily something the team which would eventually become ISRG wanted to do. And while the team knew they needed to find a way to increase the amount of page loads using HTTPS, spinning up a new CA was a daunting answer to an already ambitious challenge. Like any project in its early days, questions definitely outweighed answers:

How can we quickly increase the number of web pages using HTTPS globally? Can we change policies or practices, or do we have to build something to do it? Is it even really possible to try to make this tectonic shift for the betterment of everyone's security and privacy online?

The answer to those questions and more became "just build it." That idea led to nearly two years of work building Let's Encrypt, eventually leading to it issuing its first certificate in September 2015, opening public beta later that year.

That notion of just building it continues to drive ISRG in its mission to advance security and privacy for billions of people using the Internet every day. For Let's Encrypt, it means continuing to improve our systems to scale towards one billion active domains. For Prossimo, we're focused on building or improving software that's fundamental to the Internet operating every day—from DNS to the Linux kernel. And with Divvi Up, we're building what is the only nonprofit service focused on advancing privacy-respecting telemetry at scale. All of that work is built upon an approach that values doing the right thing.

With ten years of impact behind us, we know that the path we've taken has been made possible thanks to our community of people, funders, and supporters around the world. Looking ahead, we're confident that together we can continue to advance an Internet that's more secure and privacy-respecting for everyone, everywhere.

TEN YEARS AT A GLANCE

- **MAY 24, 2013:** ISRG is incorporated, intending to build Let's Encrypt
- **NOVEMBER 18, 2014:** Let's Encrypt is announced publicly
- **SEPTEMBER 14, 2015:** Let's Encrypt issues its first certificate
- **OCTOBER 19, 2015:** Let's Encrypt becomes publicly trusted
- **DECEMBER 3, 2015:** Let's Encrypt becomes generally available
- **MARCH 8, 2016:** Let's Encrypt issues its millionth certificate
- **JUNE 28, 2017:** Let's Encrypt issues its 100 millionth certificate
- **MARCH 11, 2019:** The ACME protocol becomes an IETF standard
- **FEBRUARY 27, 2020:** Let's Encrypt issues its billionth certificate
- **OCTOBER 26, 2020:** ISRG Board approves a privacy preserving metrics project, now Divvi Up
- **DECEMBER 9, 2020:** ISRG Board approves a memory safety project, now Prossimo
- **DECEMBER 18, 2020:** Divvi Up starts servicing COVID-19 Exposure Notification
- **OCTOBER 3, 2022:** Support for rust is merged into the Linux kernel

People powered

A NOTE FROM OUR VICE PRESIDENT

We typically open our annual report with a letter from our Executive Director and co-founder, Josh Aas, but he's on parental leave so I'll be filling in. I've run the Brand & Donor Development team at ISRG since 2016, so I've had the pleasure of watching our work mature, our impact grow, and I've had the opportunity to get to know many great people who care deeply about security and privacy on the Internet.

One of the biggest observations I've made during Josh's absence is that all 27 people who work at ISRG fall into that class of folks. Of course I was a bit nervous as Josh embarked on his leave to discover just how many balls he has been keeping in the air for the last decade. Answer: it's a lot. But the roster of staff we've built up made it pretty seamless for us to keep moving forward.

Let's Encrypt is supporting 40 million more websites than a year ago, bringing the total to over 360 million. The engineering team has grown to 12 people who are responsible for our continued reliability and ability to scale. But they're not maintaining the status quo. Let's Encrypt engineers are pushing forward our expectations for ourselves and for the WebPKI community. We've added shorter-lived certificates to our 2024 roadmap. We're committing to this work because sub-10 day certificates significantly reduce the impact of key compromise and it broadens the universe of people who can use our certs. In addition, the team started an ambitious project to develop a new Certificate Transparency implementation because the only existing option cannot scale for the future and is prone to operational fragility. These projects are led by two excellent technical leads, Aaron Gable and James Renken, who balance our ambition with our desire for a good quality of life for our teams.

Prossimo continues to deliver highly performant and memory safe software and components in a world that is increasingly eager to address the memory safety problem. This was evidenced by participation at Tectonics, a gathering we hosted which drew industry leaders for invigorated conversation. Meanwhile, initiatives like our memory safe AV1 decoder are in line to replace a C version in Google Chrome. This change would improve security for billions of people. We're grateful to the community that helps to guide and implement our efforts in this area, including Dirkjan Ochtman, the firms Tweede golf and Ferrous Systems, and the maintainers of the many projects we are involved with.

Our newest project, Divvi Up, brought on our first two Subscribers in 2023. Horizontal, a small international nonprofit serving Human Rights Defenders, will be collecting privacy-preserving telemetry metrics about the users of their Tella app, which people use to document human rights violations. Mozilla is using Divvi Up to gain insight into aspects of user behavior in the Firefox browser. It took a combination of focus and determination to get us to a production-ready state and our technical lead, Brandon Pitman played a big role in getting us there.

We hired Kristin Berdan to fill a new role as General Counsel and her impact is already apparent within our organization. She joins Sarah Heil, our CFO, Josh, and me in ISRG leadership.

Collectively, we operate three impactful and growing projects for $7 million a year. This is possible because of the amazing leadership assembled across our teams and the ongoing commitment from our community to validate the usefulness of our work. As we look toward 2024 and the challenges and opportunities that face us, I ask that you join us in building a more secure and privacy respecting Internet by sponsoring us, making a donation or gift through your DAF, or sharing with the folks you know why security and privacy matter to them.

SARAH GRAN

VP, BRAND & DONOR DEVELOPMENT

Encryption for free. For good.

EXPANDING ENCRYPTION AROUND THE WORLD

Today the Internet serves at least five billion people every day. And while user growth continues, so do the ways in which people and organizations leverage the Internet. Let's Encrypt continues to scale, serving hundreds of millions of domains—from websites to infrastructure endpoints and more.

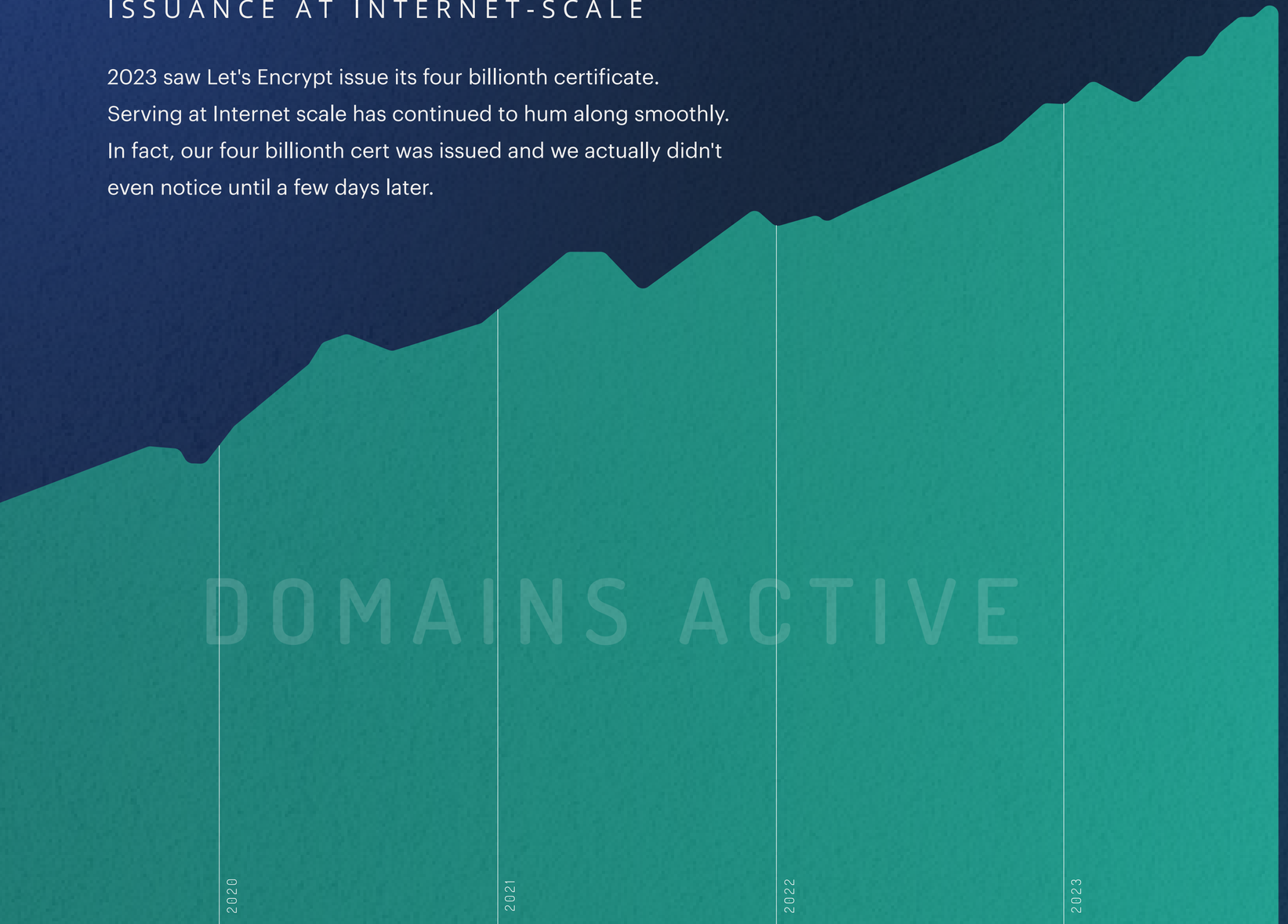
We approached our friends over at Censys to help us take a broader look at how Let's Encrypt is serving the Internet all around the world, particularly in places where the Internet is becoming a larger part of peoples' lives for the first time.

Not an issue

ISSUANCE AT INTERNET-SCALE

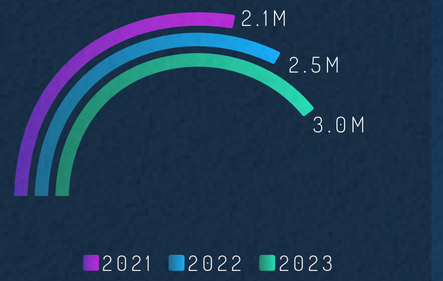
2023 saw Let's Encrypt issue its four billionth certificate. Serving at Internet scale has continued to hum along smoothly. In fact, our four billionth cert was issued and we actually didn't even notice until a few days later.

DOMAINS ACTIVE
363,516,200

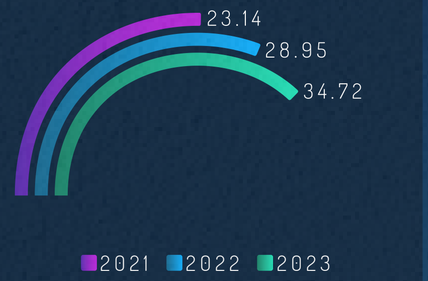


CERTIFICATES ACTIVE, YOY

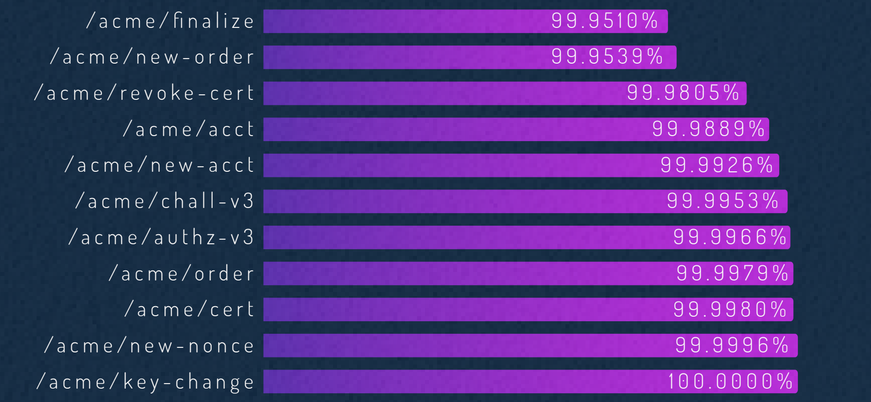
AVG. DAILY ISSUANCE, YOY



AVG. ISSUANCE PER SECOND, YOY



LET'S ENCRYPT SERVICE LEVEL INDICATORS

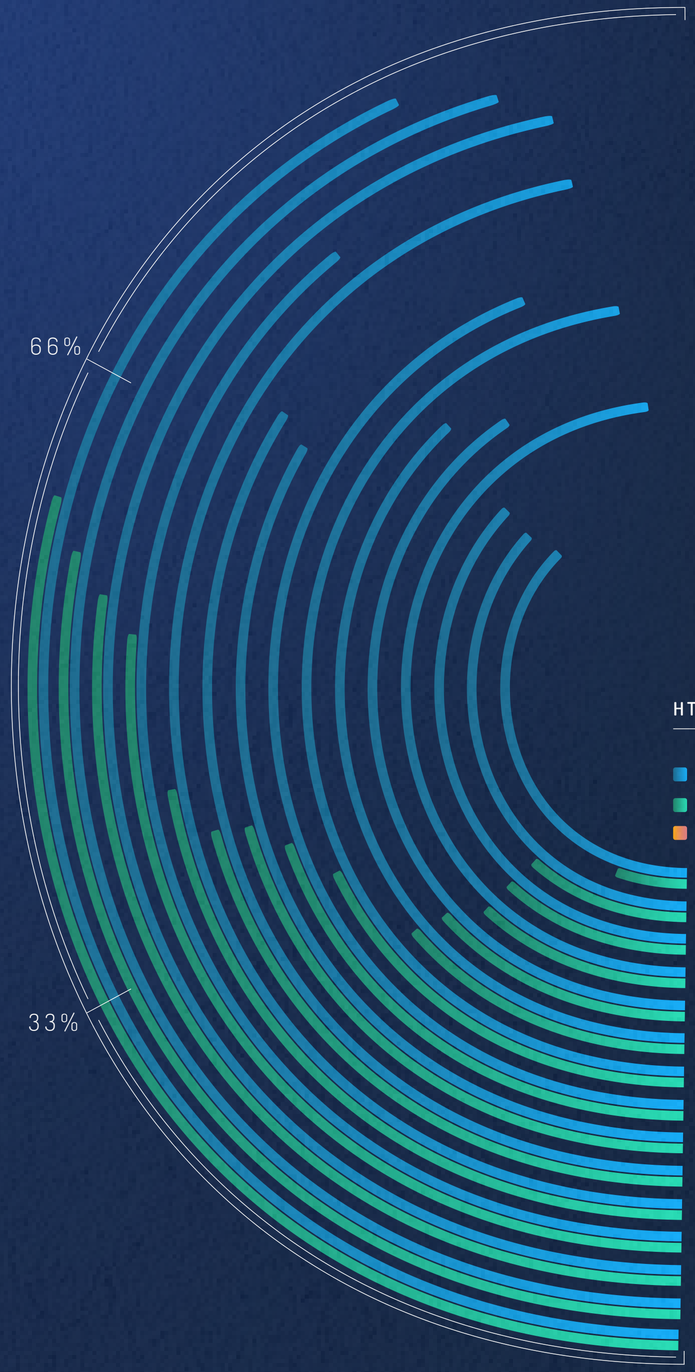


Let's Encrypt has internal Service Level Objectives (SLOs) that guide our assessment of our infrastructure's performance and health. We observe the corresponding Service Level Indicators (SLIs) on a 90-day rolling basis. These SLIs reflect the uptime across our API endpoints during a recent analysis. SLOs and SLIs inform engineering decisions like planned maintenance or timing of new features. Since the purpose of these is to serve as internal guidance, they do not constitute a promise or guarantee to external parties about the Let's Encrypt service.

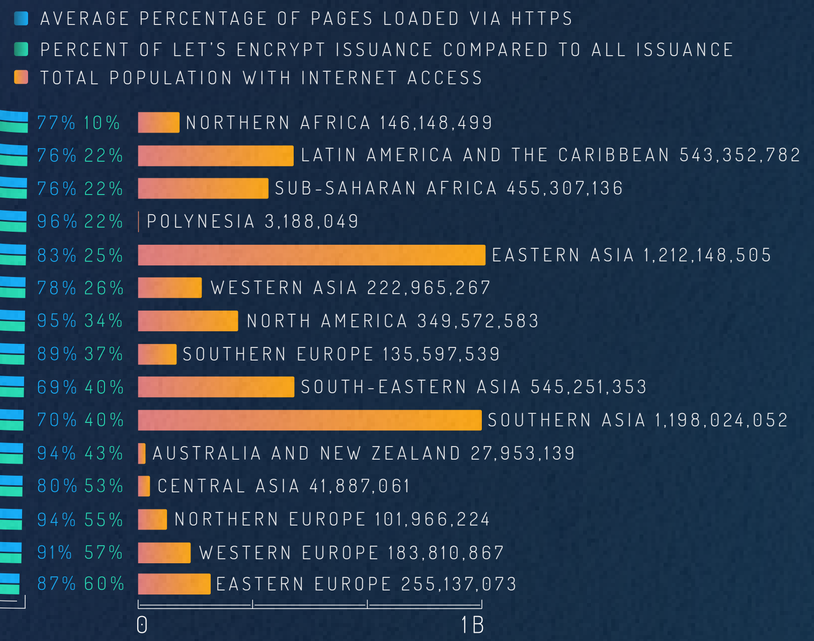
https://globally

TLS ADOPTION AROUND THE WORLD

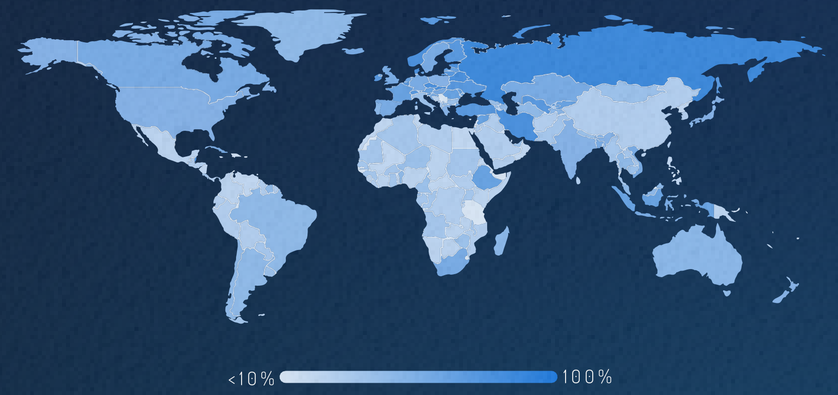
This page takes a closer look at the use of HTTPS across the world, as well as the percentage of TLS certificates issued by Let's Encrypt on average across each region. Overall, it's good news: HTTPS makes up 84% of page loads on average. That means the Internet is more secure and privacy-respecting for all of its 5.4 billion users.



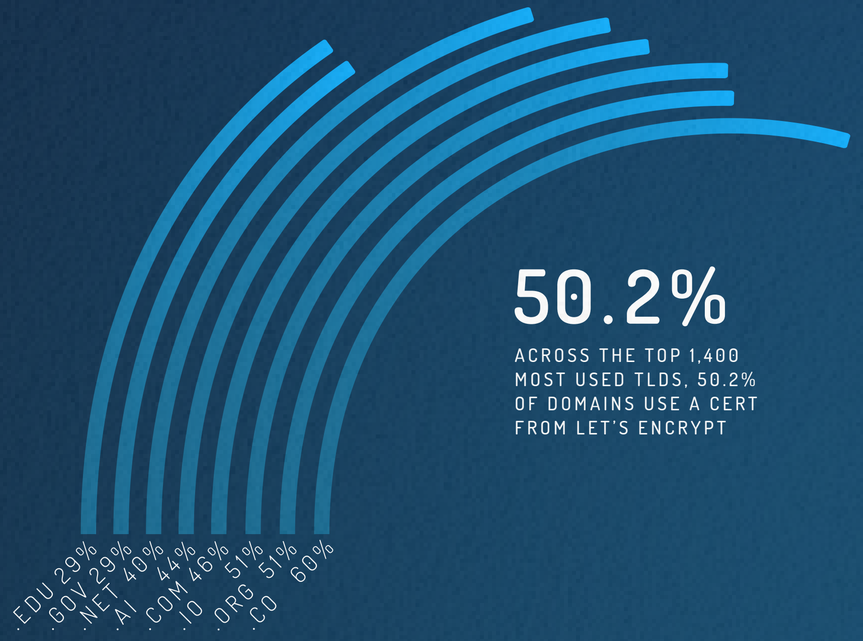
HTTPS PAGE LOADS, % TLS ISSUANCE FROM LET'S ENCRYPT, & TOTAL INTERNET USERS



PERCENT OF PAGES LOADED WITH TLS FROM LET'S ENCRYPT BY COUNTRY



LET'S ENCRYPT USAGE ON SOME COMMON TLDS



50.2%

ACROSS THE TOP 1,400 MOST USED TLDS, 50.2% OF DOMAINS USE A CERT FROM LET'S ENCRYPT

HTTPS Percent Page Loads via FIrefox SSL Ratios

Taking a look, technically.

OUR INTERNET-SCALE FOCUS

Let’s Encrypt has been focused on innovation since the beginning. That focus was necessary to bring about Internet-scale change by way of proliferating the adoption of TLS. One early example was using short certificate lifetimes of 90 days to incentivize users relying on automation for renewing certificates. This year, the team continued to push Let’s Encrypt and the Web PKI forward. The following pages have just a few examples...

ACME Renewal Information (ARI)

In March we announced ARI being live in production. ARI makes it possible for Subscribers to handle certificate revocation and renewal as easily and automatically as the process of getting a certificate in the first place.

With ARI, Let's Encrypt can signal to ACME clients when they should renew certificates. In the normal case of a certificate with a 90 day lifetime, ARI might signal for renewal at 60 days. If Let's Encrypt needs to revoke a certificate for some reason, ARI can signal that renewal needs to happen prior to the revocation. This means that when necessary, renewal can happen in an entirely automated way without disrupting subscriber services.

Without ARI, an unexpected revocation event might mean that Let's Encrypt would have to send emails to affected Subscribers, maybe those emails are read in time to avoid a service disruption, maybe they aren't, and engineers have to manually take action to trigger early renewals, possibly in the middle of the night.

Transitioning to Nomad

The Let's Encrypt Site Reliability Engineering (SRE) team spent a large part of 2023 on a major transition in how we run our microservices. Boulder, the software behind Let's Encrypt, relies on many small, separate, interlinked programs.

Previously, each of these microservices ran as a process in its own virtual machine (VM). For example, if we needed more Web Front Ends, we needed to build a new VM; even with some automation in place, this added a lot of structure and management overhead.

The team moved to a system called Nomad which automates and orchestrates running each microservice wherever there's room to do so. It also handles all of the network links between them. Overall this major transition improves the quality of life for our SRE team and improves the resiliency and agility of Let's Encrypt.

CAA Account & Method Binding

DNS governance is a topic that concerns more and more Subscribers as their need for TLS diversifies and expands. CAA, which stands for Certificate Authority Authorization, enables Subscribers to specify which Certificate Authority (CA) can issue TLS certificates for their domain(s).

This year the team shipped an extension to CAA which allows Subscribers to also specify which validation method—DNS-01, HTTP-01, or TLS-ALPN-01—can be used to demonstrate control over their domain(s). It also enables a Subscriber to specify which ACME account can be used to provision TLS.

Redis OCSP

Thousands of times per second, Internet users ask us about a certificate's current validity using the Online Certificate Status Protocol (OCSP). As we covered last year, OCSP caching is a major draw on our resources given the scale of these requests.

In 2022 the team made great strides in better handling OCSP. Previously, we handled OCSP out of our same general-purpose database and continuously updated it with refreshed copies of all certificates' status—with more than 290 million active certificates, the numbers were massive to say the least. This year, we changed to "live signing" which further improves our efficiency and resource draw. Live signing allows us to only generate a status response once we're asked, where we can then cache it in a separate database.

Looking down the path ahead

All of these technical improvements have advanced the stability, agility, and resilience of Let's Encrypt. Importantly, they also set the stage for continued advancements for Let's Encrypt and the Web PKI overall.

In 2024, we anticipate improving Certificate Transparency (CT) by taking a look at the software behind CT. CT Logs are a fundamental part of the Web PKI as they're a publicly-checkable way to confirm a certificate's validity. As a requirement of all major browsers, each Certificate Authority (CA) must publish their certificates to two CT logs. Let's Encrypt runs one of just a handful of CT logs, which supports our issuance along with submissions from most other CAs. Running CT is a major resource draw in compute, storage, and dollars. We plan to improve how we handle CT by rewriting the software—software we'll make available to anyone running a CT log.

Certificate lifetimes will also be a focus of 2024. Today Let's Encrypt issues certificates with a lifetime of 90 days. A few other CAs issue certificates with even shorter lifetimes. We plan to move forward with looking at how Let's Encrypt may be able to issue certificates with a lifetime shorter than 90 days.

On call for us all

A CLOSER LOOK AT OUR SITE RELIABILITY ENGINEERING

Let's Encrypt's Site Reliability Engineering (SRE) team runs our day-to-day operations, and builds tools to make those operations more automated and more reliable. Our on-call rotation is critical to both these parts of our job. We need to handle problems quickly, and the better our automation gets, the less often we have to do so...

Since our team runs both on-premise infrastructure and cloud-native applications, our needs span both traditional IT monitoring systems and modern observability platforms.

Most of our monitoring is based on metrics. We run the open source Prometheus software, plus a few "exporters" to interpret data from third-party products that don't offer standardized metrics. It continuously checks about 150 alert expressions we've written, firing alerts if conditions match one of those expressions. We also have some log-based monitoring, using both open source software and a popular third-party Software as a Service (SaaS) platform to watch for critical events in our logs. Finally, we have external "black box" monitoring to alert if our service is unhealthy in ways we didn't anticipate, or if our own monitoring systems are offline. Alerts are sent to both our internal chat and the on-call engineer's phone via another SaaS platform.

All teams like ours struggle to avoid "alert fatigue." We want to alert on every condition that could reduce our service levels. At the same time, we don't want to disturb our on-call engineer unless the condition is both urgent and actionable. Our team has a short weekly "alert triage" meeting to identify alerts that are too noisy or too quiet. Then, we prioritize improving those alerts over most other work. As a small team handling many complex services, it's critical for us to keep our on-call shifts tolerable.

We started paying closer attention to alert fatigue at the start of 2023, when we realized how stressful our on-call shifts had become. Over the course of the year, we've halved our average alert volume, cut our subjectively "bad" or "awful" on-call shifts by 66%, and even slightly improved our Service Level Indicators (SLIs) in the process.

> **Congratulations to ISRG on its tenth anniversary and for the growth of its Let's Encrypt program. As the Internet increases in importance to our daily lives, security has become essential and ISRG is a vital part of providing it."**

VINT CERF
VP & CHIEF INTERNET EVANGELIST
GOOGLE

Making it memory safe

MOVING TOWARDS A MEMORY SAFE INTERNET

Through our Prossimo project, we're helping address the ubiquitous problem of memory safety vulnerabilities by working to transition the Internet's critical infrastructure to memory safe code. We're also aiming to be a catalyst in the creation of memory safe alternatives to critical software in collaboration with our partners and funders.

PROSSIMO

FOR MEMORY SAFETY

Memory safety is a quality of some programming languages that prevents a specific class of vulnerabilities known as memory safety vulnerabilities. These vulnerabilities are extremely prevalent. Google and Microsoft have each reported that 70 percent or more of their vulnerabilities are a result of memory safety bugs.

What's more, agencies from the governments of the United States, Australia, Canada, Germany, Netherlands, and New Zealand published a joint report just this year that names memory safety among the top software development practices software producers should adopt. Prossimo is the only nonprofit project today leading concerted, funded, and focused efforts to eliminate memory safety vulnerabilities in the Internet's critical software.

Although this problem is widespread and impacts all of us, we believe Internet-scale change is possible and are taking an innovative approach to solving it. Our first goal is to move the Internet's security-sensitive software infrastructure to memory safe code. Much of the Internet's critical infrastructure is written in the C and C++ languages because they were the best option available for most of the Internet's history. Recent developments with memory safe languages now make a safer path possible.

We also endeavor to change people's expectations around memory safety. That starts with those maintaining Internet-scale software infrastructure. We work with maintainers whenever possible because it creates buy-in and alleviates resource concerns. Looking more broadly, our aim is to get people to fully recognize the risk and view memory safety as a requirement for software in security-sensitive roles.

Prossimo Progress

SHIFTING THIS WORK FORWARD

Recognizing the amount of work it will take to move significant portions of the Internet's C and C++ software infrastructure to memory safe code, we're tackling the transition through select initiatives. By being smart about our investments and focusing on the most critical Internet infrastructure components, we're seeing significant returns.

AV1

We're working on an AV1 decoder called rav1d, which can be used for both video and images. Our strategy is to move the C code in the dav1d decoder to Rust, while retaining the high performance assembly code. Image and video decoders have historically been a major source of exploitable memory safety vulnerabilities because they often process data from networks in complex ways. Improving memory safety for media decoders is important if we want to reduce the number of exploitable vulnerabilities people are exposed to on the Internet.

Immunant is the primary contractor for this work, with assistance from veteran codec expert Frank Bossen. They are using a strategy that's new for Prossimo - transpiling.

sudo and su

It's hard for us to imagine software that's more critical than sudo and su. These utilities mediate a critical privilege boundary on just about every open source operating system that powers the Internet. Unfortunately, sudo and su have a long history of memory safety issues. That's why we're partnering with Tweede golf and Ferrous Systems to reimplement the ubiquitous sudo and su utilities in the memory safe language Rust, ensuring they won't suffer from future memory safety vulnerabilities.

In August we announced the first stable release of sudo-rs. The sudo utility is one of the most common ways for engineers to cross the privilege boundary between user and administrative accounts in the Linux operating system. As such, its security is of the utmost importance. Chainguard's Wolfi Linux OS now includes sudo-rs and we hope that others will follow their lead.

Rustls

(0.21.9 release)

The latest release in November of a memory safe TLS implementation, Rustls, had two major new features and a number of other improvements. The first big feature is support for TLS certificates containing IP addresses. Rustls can now be used to set up TLS connections addressed by IP rather than a domain name. This was the most heavily requested feature for quite awhile and it's great to have it completed. The second big feature is support for RFC8446 C.4 client tracking prevention. This means that passive network observers will no longer be able to correlate connections.

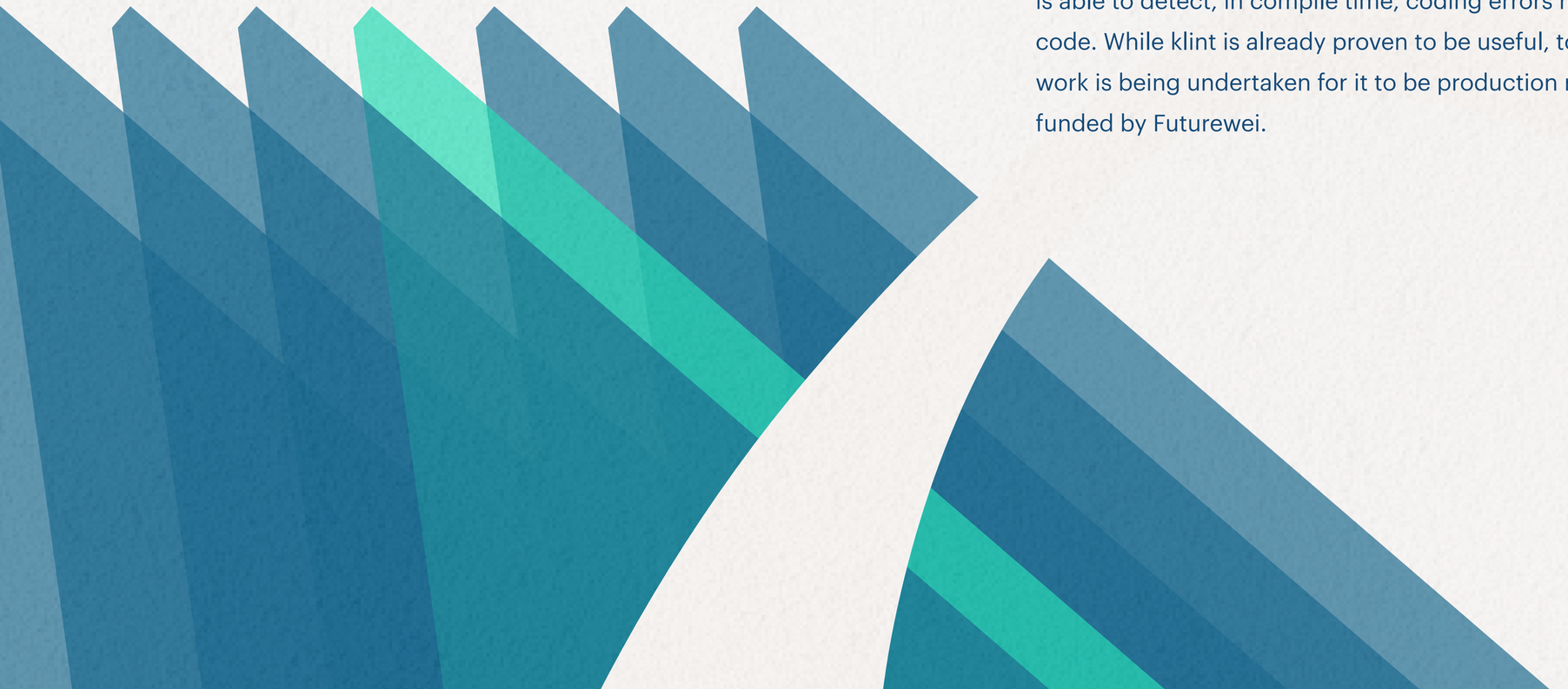
Network Time Protocol (NTP)

This year we saw ntpd-rs, a memory safe NTP implementation we supported, become ready for early adopters. This is a huge step forward for memory safety on the Internet. ntpd-rs includes a server and client, as well as full support for Network Time Security (NTS), which brings encryption and greater integrity to time synchronization. If you're running NTP services and want to improve the security of your systems, consider adopting ntpd-rs today. We worked on this initiative with the Tweede golf team as part of their Pendulum project and they're now the long-term maintainer of ntpd-rs. The initiative was generously funded by Cisco and Amazon Web Services.

Rust in the Linux kernel

With Prossimo support, Miguel Ojeda continues work on his Rust for Linux project, making great progress this year.

Klint is a Rust tool Gary Guo created that will benefit our work with the Linux kernel. Klint is able to detect, in compile time, coding errors related to atomic contexts in Rust kernel code. While klint is already proven to be useful, to date it is largely a prototype and more work is being undertaken for it to be production ready. This initiative was generously funded by Futurewei.



Behind the work

BUILDING CODE, BUILDING MOMENTUM

Our Prossimo work is in no way done in a silo. We're joined in our aims and undertakings by dedicated memory safety advocates and maintainers, and the funders who recognize the value of our work and make it possible.

Tectonics

Prossimo isn't alone in this work to move the Internet toward a more memory safe future. We had the honor of bringing together a group of memory safety advocates at our Tectonics convening in San Francisco on November 2 of this year. We welcomed keynotes by Window Snyder of Thistle Technologies, David Weston of Microsoft, and Doug Gregor of Apple about this critical Internet security topic. Fiona Krakenbürger of Sovereign Tech Fund delivered incisive closing remarks. We're grateful to everyone who joined us.

Attendees participated in breakout sessions covering:

1) Facilitating adoption of memory safe code for Internet critical infrastructure
2) Memory safety roadmaps for organizations
3) Facilitating the inclusion of Rust in operating systems
4) Improving trust in Rust dependency trees

Each group focused on tackling questions around memory safety adoption, shifting emphasis from determining 'why does this problem exist' to 'how are we going to fix it.'

Financially supported by the Ford Foundation, Google, Tweede golf, and Heroku, we set out to make the conversation a "2.0". The goal was to move past the discussion of the problem to focus on solutions. We were pleased with how many stories of experience were shared; it was a reminder of how much great progress has already been made.

There were perspectives coming from practitioners, policy makers, advocacy folks, and people in a position to make engineering priority decisions. Participants really valued hearing how others are using their skills and energy to tackle this enormous challenge.

"This was the best conference I have been to in a long time. Sitting in a cross industry group of absolute experts talking about how to solve a common problem was inspiring. I came back more convinced than ever we will solve this problem."

DAVID WESTON
VICE PRESIDENT OF ENTERPRISE AND OS SECURITY
MICROSOFT

Improving memory safety is not just a technological challenge. The day's conversations were a good reminder that people are at the heart of changing how security-sensitive software is written, used, and thought about.

Funders

The strides we've taken toward creating a more memory safe Internet wouldn't be possible without our generous funders, who recognize and believe in the importance of this work.

Our Prossimo project received the following new support this year:

Amazon Web Services

In May we announced that Amazon Web Services (AWS) will continue its support of Prossimo through a gift of $1 million. AWS has long supported ISRG's mission through sponsorships of projects such as Let's Encrypt and its early contributions to Prossimo's curl initiative. This new gift is supporting the development of four of our memory safety initiatives, including our memory safe AV1 decoder, rav1d, and our work rewriting sudo and su in Rust. It also will help further our efforts with Rustls and the development of ntpd-rs. We're grateful for AWS's longtime commitment to helping ISRG and its projects build a more secure and privacy-respecting Web.

"At AWS, security is job zero and we are constantly looking for ways to help us and our customers operate more securely. With this funding, we're furthering ISRG's mission to build a more memory safe internet through the creation of new solutions for securing critical software tools. Investing in open source communities is essential to their long-term sustainability so they can continue to help tackle complex problems like memory safety."

DAVID NALLEY
HEAD OF OPEN SOURCE STRATEGY & MARKETING
AMAZON WEB SERVICES

Sovereign Technology Fund

We announced in July that Sovereign Tech Fund is supporting our Prossimo project with $1.5 million. This funding will cover work on three memory safety initiatives, Rustls, rav1d, and DNS. We applaud the Sovereign Tech Fund and the German government for recognizing the connection between strong, well-supported digital infrastructure and innovation and economic growth.

"The memory safety work that the Internet Security Research Group does with Prossimo is absolutely essential. It exemplifies the digital infrastructure and open source ecosystem the Sovereign Tech Fund wants to support. By investing in making TLS, the AV1 media decoder, and a DNS resolver more secure, we're acting in the public interest by improving the security of everyone using the internet, from individuals to companies and governments. Together, we're safeguarding our shared digital infrastructure for the common good."

FIONA KRAKENBÜRGER
CO-FOUNDER
SOVEREIGN TECH FUND

OpenSSF

In September, we announced that our Prossimo project is receiving $530,000 in funding from the OpenSSF's Alpha-Omega project. Thanks to OpenSSF's generous support, Prossimo will continue to advance the functionality and scalability of the Rustls TLS library and the Rust for Linux effort. This work also furthers the mission of OpenSSF's Alpha-Omega project, to protect society by improving the security of open source software.

"As a memory-safe language, Rust plays a pivotal role in fortifying critical software infrastructure. Alpha-Omega is proud to support Prossimo's efforts to enhance the Rustls cryptographic library and bolster Rust's integration within the Linux kernel."

MICHAEL SCOVETTA
CO-LEAD
OPENSSF ALPHA-OMEGA

Insights without infringement

PRIVACY-PRESERVING METRICS COLLECTION

Divvi Up is a system application owners can use to collect app users' metrics while respecting their privacy. In this way, Divvi Up makes it possible for web browsers, mobile applications, or websites to gain valuable insights about a user population without compromising individual privacy. This year, we've been focused on preparing Divvi Up for its first subscribers.

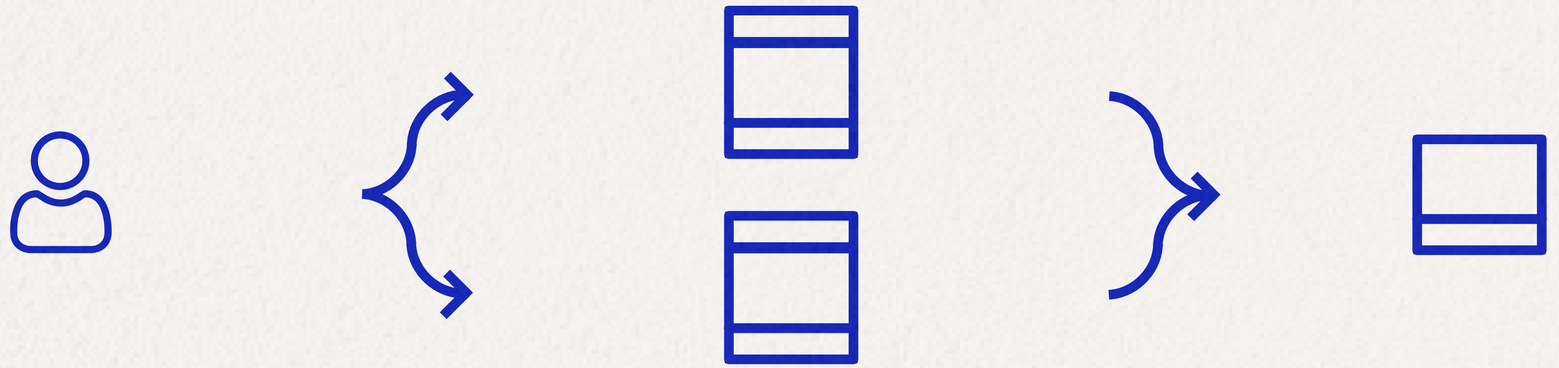
Divvi Up

Data divided. Data secured.

How it works

A SIMPLE SCHEME. COMPLEX MATH.

Divvi Up takes a user-generated metric from a mobile device, web browser, or other application, and divides the metric into two encrypted shares as it leaves the origin. One half of that metric is sent to a Divvi Up server, the other to a third-party server. When an application owner queries an aggregate statistic of its users, Divvi Up combines the divided metrics from all users and produces a privacy-preserving aggregate.



A USER-GENERATED VALUE

DIVIDE THE VALUE

TWO NON-COLLUDING SERVERS

COMBINE AGGREGATES

ANONYMIZED INSIGHT

Many types of applications—from mobile and desktop apps to websites—generate metrics about their users. These metrics are valuable for application owners because they are the basis for insights into users' behavior. Normally an application would send all user metrics back to the app owners, either directly or through a middle-entity. Users simply have to trust that app owners will respect their stated privacy and security policies.

Stated policy, however, is insufficient as a privacy safeguard. Once an app owner has user data, privacy policies can be violated either intentionally or accidentally. The mere possibility of privacy violations can erode trust in apps, making users less likely to want to engage. In addition, the presence of personally identifiable information is a liability that more organizations are worrying about since it can be unintentionally leaked or stolen in a breach.

Technology to bolster peoples' privacy while using apps is becoming a stronger area of research and development. A paper published in 2017 by Henry Corrigan-Gibbs and Dan Boneh of Stanford University demonstrated a novel approach to privacy preserving metrics. That paper set a foundation for how to gain insights about a population of app users without infringing upon the privacy of any individual in that population.

“If data exists it's a risk.”

RAPHAEL MIMOUN
FOUNDER, CURRENT PROGRAMS LEAD
HORIZONTAL

We built upon this research to develop Divvi Up. We operated an early version of this system beginning in late 2020 to provide privacy-respecting metrics for COVID-19 exposure notification apps in partnership with Apple, Google, National Cancer Institutes, and The MITRE Corporation. Today, ISRG is continuing to operationalize Divvi Up for a broader set of use cases.

One of the key elements needed to make Divvi Up a successful self-serve tool for app owners is the ability to spin up new metrics collection without too much time investment or the involvement of a Real Live Human. The Divvi Up management console is under construction to achieve just that. We've sketched out a flow for new subscribers to determine what metrics they want to collect and over what period of time. We’re currently developing the management console so it can help subscribers get up and running quickly. It will enable Subscribers to efficiently get metrics that can provide valuable insight to inform application design and functionality decisions.

Writing a standard

NEARING AN IETF STANDARD

Since we started building Divvi Up, we've shepherded eight drafts of the Distributed Aggregation Protocol (DAP) through the Internet Engineering Task Force (IETF) alongside the development of our own implementations of that protocol. We're creating a service that will reduce the unique information application users expose about themselves and their behaviors by turning individual data points into aggregate, anonymized metrics.

Divvi Up has been running DAP-02 and DAP-04 for some time now. We are looking to land on DAP-07 shortly as a long-running version upon which we will build our production service.

The biggest difference between DAP-04 and DAP-07 is an improvement in the performance of the aggregation subprotocol thanks to an approximately 50% reduction of network requests.

This efficiency gain will decrease the cost of running Divvi Up and improve our ability to scale. We are collaborating with initial partners to ensure there is an ecosystem of providers who are all interoperable on DAP-05.

Our first production users

HORIZONTAL & FIREFOX

This year we publicly announced our first two production users of Divvi Up, Human Rights Defenders oragnization Horizontal, and Mozilla's browser, Firefox.

Human Rights Defenders At Horizontal

Divvi Up's first production user, Horizontal, is a nonprofit organization supporting frontline defenders, activists, and journalists through digital security and tool development.

As Horizontal says, "While the Internet has connected us, amplified the voices of the most vulnerable, and helped build movements, it has also become a tool to survey, monitor, and repress." What's more, even for organizations seeking to protect and advance user privacy and security such as ISRG and Horizontal, technologically doing so can be difficult, if not impossible.

Such was the case for Horizontal's application Tella, a tool that enables users to safely and securely collect and store information, making it easier and safer to document human rights violations and collect data. Horizontal's Founder and current programs lead, Raphael Mimoun, told us, "We have reached a point with Tella where it is mature. We know we need to step up our game and learn about how people are using it." While the team would have benefited from telemetry of the app's performance, there previously wasn't an easy method to collect telemetry without accessing some sort of user information. When it comes to collecting any user data, Raphael continued, "if data exists, it's a risk."

Horizontal is a team of 10 located in seven countries around the world. Juan Dans, software engineer, set up Divvi Up in close collaboration with the Divvi Up team. "There was a process of learning the tool. At first, I approached it as a product I could implement but I realized it is something that was still really hands-on developing, so it needed to be a hands-on collaborative process," said Juan. "At the end, we had two teams working together in the same way." This collaboration led to learnings for both parties; learnings we've taken forward for both Divvi Up and the development of the IETF standard, Distributed Aggregation Protocol (DAP).

We at ISRG are thrilled Horizontal is among the first users of Divvi Up on what we hope is a journey to wide-scale adoption of privacy-preserving metrics. "It was extremely exciting to know that we are working on something totally new, and working with an organization like the one who has a track record of building great things like Let's Encrypt," said Raphael.

Firefox

Mozilla will be deploying our Divvi Up privacy-preserving metrics collection technology in Firefox. As a browser that keeps its users' privacy at the forefront, Firefox is an ideal partner for an early deployment of Divvi Up.

Collecting user metrics such as the relative frequency of visits to different web pages helps Firefox engineers identify the most important bugs to fix and features to optimize, and with Divvi Up to de-identify and aggregate the collected data, this process will also respect the privacy of Firefox users.

Our engineers collaborated with Firefox engineers and other key contributors over the last two years to develop the Distributed Aggregation Protocol (DAP) specification in the Internet Engineering Task Force (IETF), which serves as the backbone for Divvi Up. We're excited to see this technology deployed on such a broad stage as Mozilla's Firefox.

"Our objective at Mozilla is to develop viable alternatives to the things that are wrong with the internet today and move the entire industry by demonstrating that it's possible to do better. In the short term, these technologies will help us keep Firefox competitive while adhering to our longstanding principles around sensitive data. Over the long term, we want to see these kinds of strong privacy guarantees become the norm, and we will continue to work towards such a future"

BOBBY HOLLEY
CTO, FIREFOX
MOZILLA

It's all in the details

PEOPLE, FUNDERS, & FINANCIALS

Although Let's Encrypt issued its first certificate in 2015, it was nearly two years of work via ISRG to get to that point. Here's a closer look at the nonprofit organization behind our impact.

ISRG

Internet Security Research Group

Security & privacy for all

LETTER FROM ISRG BOARD CHAIR, CHRISTINE RUNNEGAR

I joined the Board of Internet Security Research Group (ISRG) in 2018 and became Board Chair last year, 2022. In those five years I've been honored to witness and be a part of ISRG providing a trusted, reliable and sustainable home for public-benefit digital infrastructure projects. As ISRG celebrates the 10th anniversary of its founding, I wanted to reflect on our impact.

ISRG has significantly enhanced the security and privacy of the Internet for users all over the world, through its Let's Encrypt certificate authority. Today, we almost take for...

granted that websites will use HTTPS to protect our interactions, and browsers have adapted to that reality by switching from notifying users when a website uses HTTPS to when it doesn't. Ten years ago, less than one third of websites were using HTTPS, even websites that handled personal data.

Let's Encrypt was a game-changer for Internet security for three simple reasons: websites could obtain SSL/TLS certificates without charge, using an automated process, and from a trusted source supported by the community as a provider of public-benefit Internet infrastructure for anyone in the world. Its great success can also be attributed to ISRG's ability to rapidly scale up its services, so that today Let's Encrypt provides certificates to more than 300 million websites.

Further, ISRG is all about community and ensuring that open-source Internet security software is used, maintained and secure. ISRG has shown that public-interest (or public-benefit) organizations provide societal value well above and beyond their individual achievements. Let's Encrypt has inspired other Internet security open-source efforts like Sigstore, an open-source initiative to provide trusted authenticity of open-source software. It has inspired commercial operators to offer the same services to the public, free and automated certificates, and has helped ensure overall trust in the digital certificate ecosystem.

ISRG's impact on the Internet does not stop there.

Through Prossimo, ISRG is on the leading edge of efforts to reduce security vulnerabilities in critical Internet infrastructure caused by memory-unsafe code, by working with the open-source community to develop new software using memory-safe programming languages. One notable example is the work on Rustls, a memory-safe implementation of the TLS protocol. TLS is widely used all over the Internet to encrypt communications, including websites, email, messaging and video conferencing so an exploited vulnerability due to lack of memory safety could cause wide-scale harm.

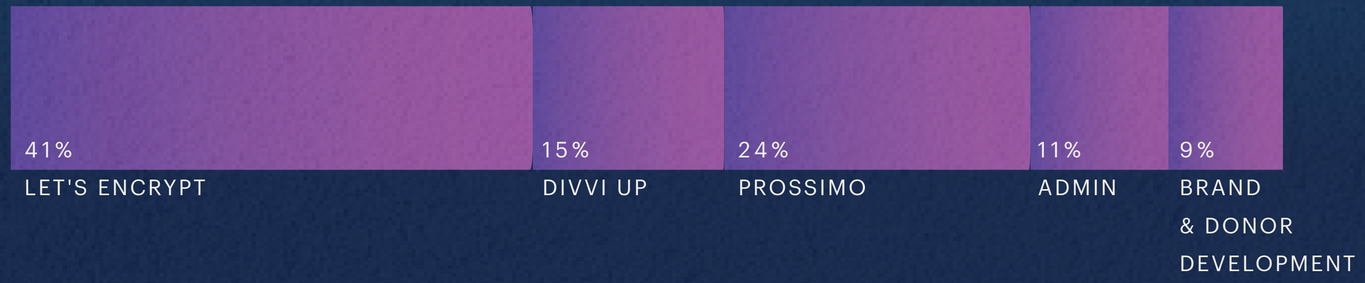
Divvi Up emerged from the work that ISRG and partners undertook to collect and analyze aggregate COVID-19 exposure notification app metrics. Through Divvi Up, ISRG will provide a more secure and privacy-respecting way for online services to collect user metrics that will hopefully help put an end to pervasive online tracking.

I'm grateful to be the Board Chair of this critical nonprofit as we celebrate the milestone of our 10th anniversary. Given all ISRG has accomplished in just this first decade, I look forward to seeing the many years ahead of their continued work to make the Internet more secure for everyone across the globe.

Financials

REVENUE

EXPENSE



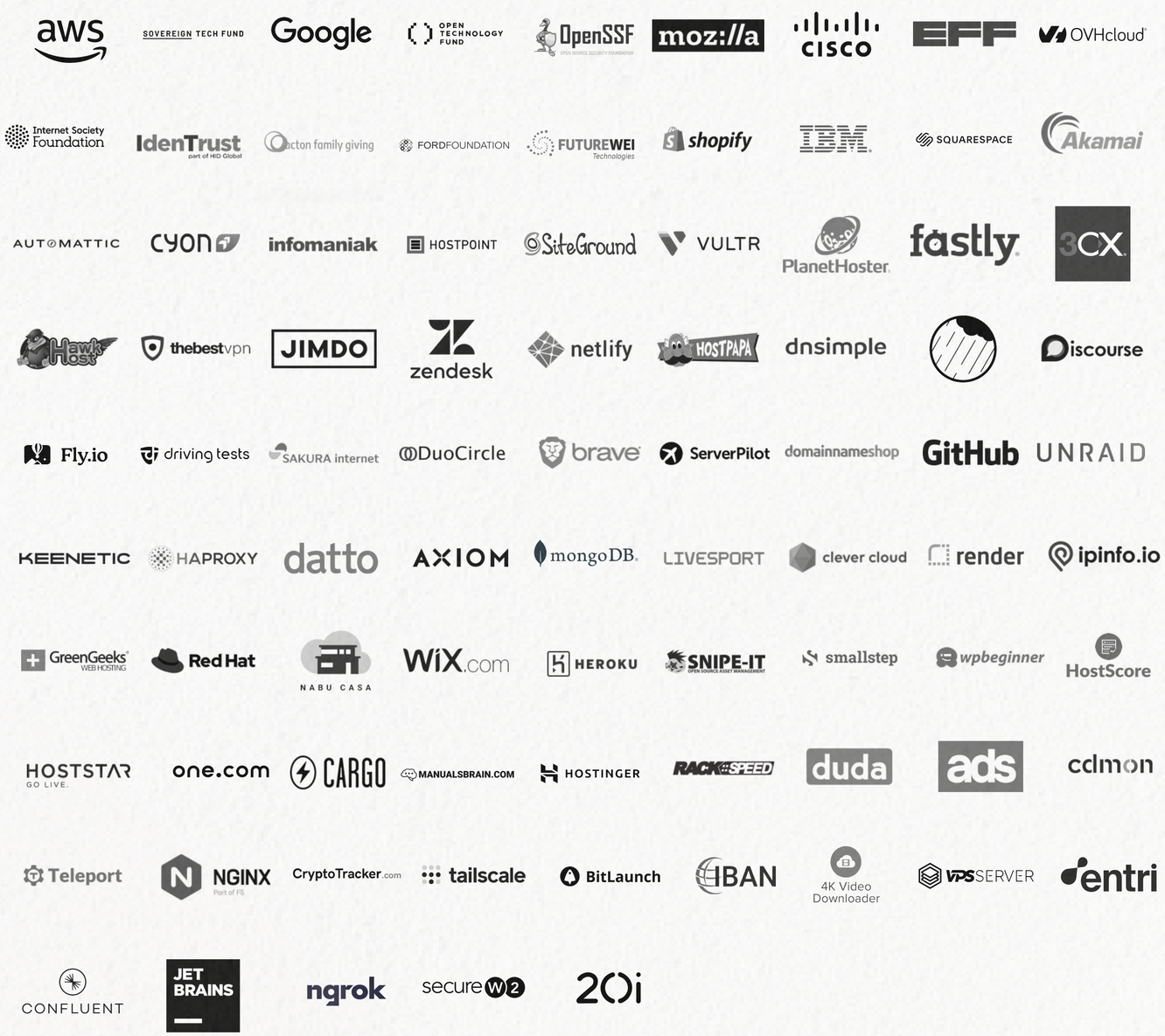
PERCENTAGES BASED ON UNAUDITED FINANCIAL JAN-OCT 2023

> **Vision combined with execution can make a big impact in the world, and ISRG has done just that."**
>
> **ALEX POLVI**
> FOUNDER
> CORE-OS

Funders

We are proud to have received funding from a broad and truly global group of funders. And while there are more than 80 logos on this page, there are hundreds of people across these organizations who make our impact possible. We're grateful for these new funders for coming on board or increasing their funding in 2023:

Sovereign Tech Fund
OpenSSF
Internet Society Foundation
IBM
Squarespace
IBAN
4k Video Downloader
VPS Server
Entri
Confluent
ngrok
securew2
20i



Board & Staff

BOARD OF DIRECTORS

AANCHAL GUPTA
INDEPENDENT

CHRISTINE RUNNEGAR
BOARD CHAIR, INDEPENDENT

DAVID NALLEY
AMAZON WEB SERVICES

JENNIFER GRANICK
INDEPENDENT

J. ALEX HALDERMAN
UNIVERSITY OF MICHIGAN

JOSH AAS
INTERNET SECURITY RESEARCH GROUP

ERICA PORTNOY
ELECTRONIC FRONTIER FOUNDATION

PASCAL JAILLON
OVHCLOUD

RICHARD BARNES
CISCO

VICKY CHIN
MOZILLA

STAFF

AARON | SOFTWARE ENGINEER
AMEER | SOFTWARE ENGINEER
ANDREW | SOFTWARE ENGINEER
BRAD | SITE RELIABILITY ENGINEER
BRANDON | SENIOR SOFTWARE ENGINEER
CARRISSA | PEOPLE MANAGER
DAN | DIRECTOR BRAND & DONOR DEVELOPMENT
DAVID | SOFTWARE ENGINEER
JACOB | SOFTWARE ENGINEER
JAMES | SITE RELIABILITY ENGINEER
J.C. | SITE RELIABILITY ENGINEER
JOSH | EXECUTIVE DIRECTOR
KIEL | SITE RELIABILITY ENGINEER
KRISTIN | GENERAL COUNSEL
KRUTI | SITE RELIABILITY ENGINEER
LENA | SITE RELIABILITY ENGINEER
MATTHEW | SITE RELIABILITY ENGINEER
MEGAN | BRAND & DONOR DEVELOPMENT SPECIALIST
OLENA | FINANCE MANAGER
PHIL | SITE RELIABILITY ENGINEER
PRESTON | SITE RELIABILITY ENGINEER
SAMANTHA | SOFTWARE ENGINEER
SARAH | VP BRAND & DONOR DEVELOPMENT
SARAH | CHIEF FINANCIAL OFFICER
SARAH | BRAND & DONOR DEVELOPMENT SPECIALIST
TIM | SITE RELIABILITY ENGINEER

Help us build a better Internet

SUPPORT OUR WORK

Thanks to our staff, community, users, sponsors, grantmakers, and individual donors, ISRG and its projects are building a more secure and privacy-respecting Internet for everyone, everywhere.

ISRG Internet Security Research Group

Let's Encrypt

PROSSIMO

Divvi Up

The mission of Internet Security Research Group (ISRG) is to reduce financial, technological, and educational barriers to secure communication over the Internet. ISRG is a California public benefit corporation, recognized by the IRS as a tax-exempt organization under Section 501(c)(3).

For more on our work, visit: https://abetterinternet.org