ISRG Internet Security Research Group

Let's build a better Internet

2022 ANNUAL REPORT

https://abetterinternet.org

A home for critical infrastructure

INTERNET SECURITY RESEARCH GROUP

Internet Security Research Group (ISRG) is the nonprofit behind Let's Encrypt, Divvi Up, and Prossimo. Since 2013, we've built and fostered Let's Encrypt to be the world's largest Certificate Authority.

2022 saw ISRG projects reach new heights in terms of scale and impact: from Let's Encrypt issuing its three billionth certificate to Prossimo supporting the efforts to get Rust into the Linux kernel.

Let's Encrypt

Divvi Up
Data divided. Data secured.

PROSSIMO
FOR MEMORY SAFETY

Contents

Agility and resiliency at scale

A NOTE FROM OUR EXECUTIVE DIRECTOR

The past year at ISRG has been great and I couldn't be more proud of our staff, community, funders, and other partners that made it happen. Let's Encrypt continues to thrive, serving more websites around the world than ever before with excellent security and stability...

JOSH AAS
EXECUTIVE DIRECTOR

A particularly big moment was when Let's Encrypt surpassed 300,000,000 websites served. When I was informed that we had reached that milestone, my first reaction was to be excited and happy about how many people we've been able to help. My second reaction, following on quickly after the first, was to take a deep breath and reflect on the magnitude of the responsibility we have here.

The way ISRG is translating that sense of responsibility to action today is best described as a focus on agility and resilience. We need to assume that, despite our best efforts trying to prevent issues, unexpected and unfortunate events will happen and we need to position ourselves to handle them.

Back in March of 2020, Let's Encrypt needed to respond to a compliance incident that affected nearly three million certificates. That meant we needed to get our subscribers to renew those three million certificates in a very short period of time or the sites might have availability issues. We dealt with that incident pretty well considering the remediation options available, but it was clear that incremental improvements would not make enough of a difference for events like this in the future. We needed to introduce systems that would allow us to be significantly more agile and resilient going forward.

Since then we've developed a specification for automating certificate renewal signals so that our subscribers can handle revocation/renewal events as easily as they can get certificates in the first place (it just happens automatically in the background!). That specification is making its way through the IETF standards process so that the whole ecosystem can benefit, and we plan to deploy it in production at Let's Encrypt shortly. Combined with other steps we've taken in order to more easily handle renewal traffic surges, Let's Encrypt should be able to respond on a whole different level the next time we need to ask significant numbers of subscribers to renew early.

This kind of work on agility and resilience is critical if we're going to improve security and privacy at scale on the Web.

Our Divvi Up team has made a huge amount of progress implementing a new service that will bring privacy respecting metrics to millions of people. Applications collect all kinds of metrics: some of them are sensitive, some of them aren't, and some of them seem innocuous but could reveal private information about a person. We're

making it possible for apps to get aggregated, anonymized metrics that give insight at a population level while protecting the privacy of the people who are using those apps. Everybody wins - users get great privacy and apps get the metrics they need without handling individual user data. As we move into 2023, we'll continue to grow our roster of beta testers and partners.

Our Prossimo project started in 2020 with a clear goal: move security sensitive software infrastructure to memory safe code. Since then, we've gotten a lot of code written to improve memory safety on the Internet.

We're ending the year with Rust support being merged into the Linux kernel and the completion of a memory safe NTP client and server implementation. We're thrilled about the potential for a more memory safe kernel, but now we need to see the development of drivers in Rust. We're particularly excited about an NVMe driver that shows excellent initial performance metrics while coming with the benefit of never producing a memory safety bug. We are actively working to make similar progress on Rustls, a high-performance TLS library, and Trust-DNS, a fully recursive DNS resolver.

"We're thrilled about the potential for a more memory safe kernel, but now we need to see the development of drivers in Rust."

All of this is made possible by charitable contributions from people like you and organizations around the world. Since 2015, tens of thousands of people have given to our work. They've made a case for corporate sponsorship, given through their DAFs, or set up recurring donations. That's all added up to more than $17M that we've used to change the Internet for nearly everyone using it. I hope you'll join these people and support us financially if you can.

JOSH AAS
EXECUTIVE DIRECTOR

Internet scale by the numbers

POWERING TLS ON THE INTERNET

2022 saw two major milestones for Let's Encrypt: the issuance of our three billionth cert and reaching 300 million active domains. Now more than ever, Let's Encrypt is behind TLS all over the Internet.

Let's Encrypt

IMPACT ON THE WEB

As of November 1, 2022, Let's Encrypt provides TLS to over 309 million domains via 239 million active certificates. Let's Encrypt usage grew by more than 33 million domains in 2022.

2022 DAILY ISSUANCE

1.8M	2.5M	3.1M
MIN	AVG	MAX

CERTS ISSUED SINCE 2015

3,078,399,255

ACTIVE CERTIFICATES

239,710,300

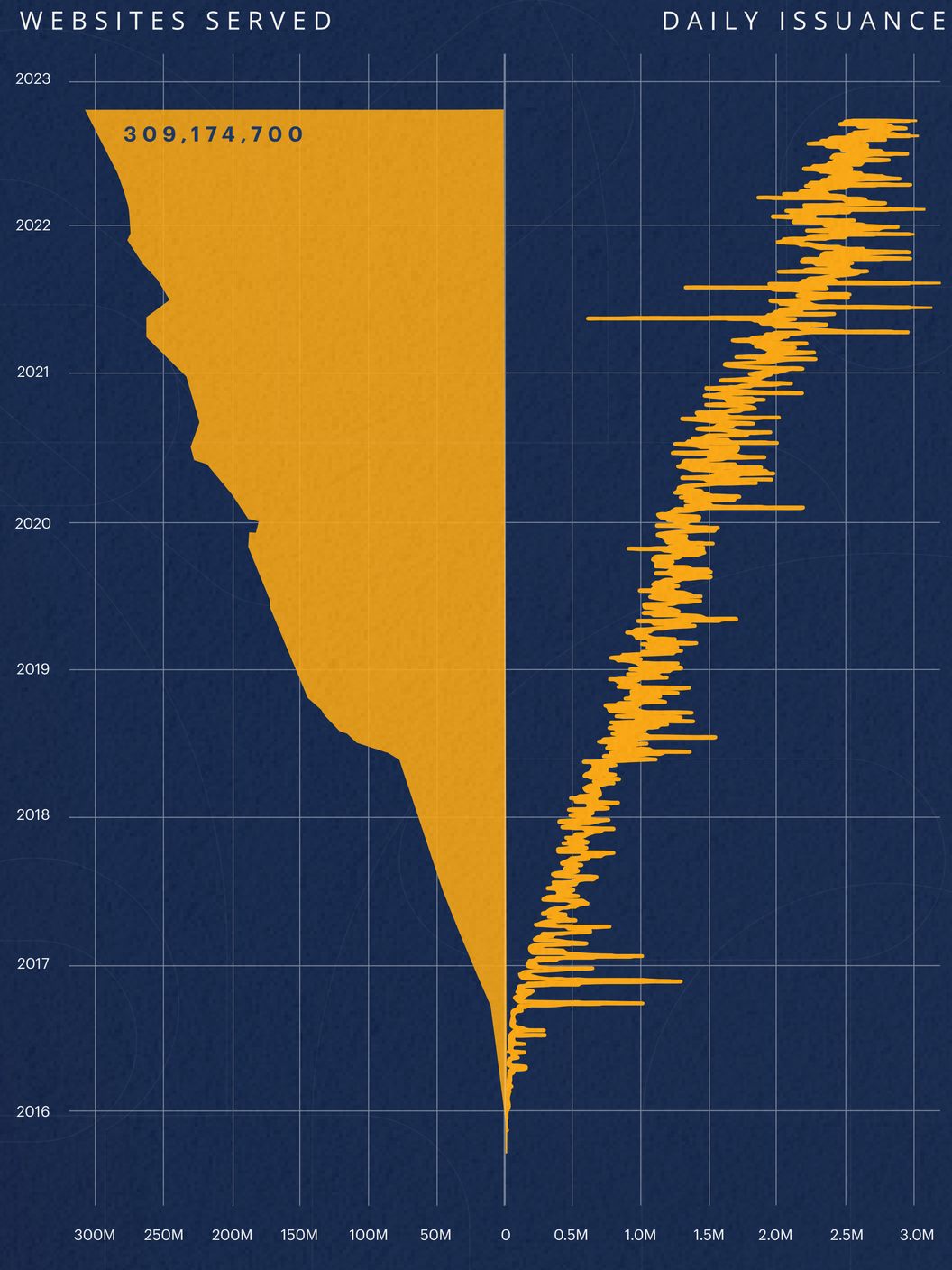
REGISTERED DOMAINS

99,496,600

82% WEB PAGES LOADED BY FIREFOX USING HTTPS, GLOBALLY

30 CERTIFICATES ISSUED PER SECOND ON AVERAGE

> **"LET'S ENCRYPT IS A CRITICAL, YET FREQUENTLY UNNOTICED, PART OF THE PUBLIC COMMONS THAT KEEPS THE INTERNET SAFE AND SECURE FOR EVERYONE."**
>
> **NADIA ASPAROUHOVA**
> AUTHOR | WORKING IN PUBLIC



Big numbers are just the beginning

CACHING OCSP REQUESTS AT MASSIVE SCALE

We're pretty used to big numbers at Let's Encrypt: today more than 300,000,000 websites have encrypted communications thanks to Let's Encrypt—and we issued our 3,000,000,000 cert just this fall.

But behind these mind-boggling numbers are a world of stats and figures that our engineers think about every day to bolster the reliability and agility of Let's Encrypt.

BUILDING OUR OWN OCSP CACHING LAYER WITH REDIS

For most of 2022, one focus of our Site Reliability Engineers and Developers has been improving how Let's Encrypt manages caching Online Certificate Status Protocol (OCSP) responses. At the start of this year 98-99% of our OCSP traffic was handled by our CDNs. But what happens when a CDN has an issue resulting in Let's Encrypt being required to take some of that load?

Since Let's Encrypt serves 300 million domains, we cache around 100,000 OCSP requests every second. Historically, Let's Encrypt could cache about 6% of this traffic on its own. But were we to experience traffic much higher than that, we'd risk Let's Encrypt falling over. Not an ideal situation for us, or the Internet.

The team has dramatically improved our ability to serve OCSP responses by deploying Redis as an in-memory caching layer that helps protect our database. The first test was to cache 1/16th of the responses. That initial test handled 12,500 requests per second. Successive tests ratcheted up to 1/8th, then 1/4th, then 1/2, then 100%.

Overall, this improvement means that Let's Encrypt is more reliable today than it's ever been—and that we have one more mind-bending stat under our belt.

Millions upon millions of domains

LET'S ENCRYPT AND THE BUSINESS-CRITICAL PATH

When Let’s Encrypt first began issuing certificates, the need was fairly straightforward: to provide TLS for websites that simply didn’t have a TLS certificate. Since then, the need to easily manage and obtain certificates at scale has exploded. And with it, the importance of Let’s Encrypt serving as critical infrastructure for the Internet—from managing TLS for millions of hosted domains to multicloud database services.

Here’s a closer look at two ways Let’s Encrypt helps secure the Web.

LET'S ENCRYPT AND MONGODB

OVHcloud and MongoDB use of Let's Encrypt exceeds millions of TLS certificates. MongoDB's managed multicloud database service, called Atlas, uses Let's Encrypt certificates to secure the connection between customers' applications and MongoDB databases, and between service points inside the platform.

MongoDB's diverse customer roster means they support a wide variety of languages, libraries, and operating systems. Consequently, their monitoring is quite robust. Over the years, MongoDB has become a helpful resource for Let's Encrypt engineers to identify edge case implementation bugs. Their ability to accurately identify issues early helps us respond efficiently; this is a benefit that ripples out across our diverse subscribers all over the Web.

> **One thing that I appreciate about Let's Encrypt is that you've always been extremely transparent on your priorities and your roadmap vision. In terms of the technology and your telemetry, this is an evolution; where you are today is far better than where you were two years ago. And two years ago you were already head and shoulders above almost every peer in the industry."**

KENN WHITE
SECURITY PRINCIPAL
MONGODB

“Just click and it works."

GUILLAUME MARCHAND
TECHNICAL TEAM LEAD
OVHCLOUD

LET'S ENCRYPT AND OVHCLOUD

OVHcloud, the largest hosting provider in Europe, has used Let’s Encrypt for TLS certificates since 2016. They’ve provisioned tens of millions of certificates for their shared hosting customers.

They first started looking into using Let’s Encrypt certificates because the team saw a need for the protection provided by TLS for every customer (remember, way back five years ago, when that wasn’t just a thing everybody did?).

> “Our goal was to deliver TLS simply. We didn’t want to have to write a tutorial for our customers to upload a cert, but instead just click and it works."
> Guillaume Marchand, OVHcloud’s Technical Team Lead.

Getting a TLS certificate is on the critical path to onboarding a shared hosting client, so monitoring is a big part of OVHcloud’s success with Let’s Encrypt. They set up monitoring at every step in the delivery process: requesting the certificate, asking for challenges, waiting for validation, and requesting certificate creation. They also keep an eye on how long it takes to get a certificate (“it’s really fast”). OVHcloud also monitors our status page to stay apprised of our operational status.

Over 10,000 certificates are issued from Let’s Encrypt to OVHcloud every day. As the company continues to expand into North America, they predict that number will grow. The initial and ongoing work done by the OVHcloud team ensures that TLS will be a simple and reliable aspect of their service.

A revocation evolution

A NEW LIFE FOR CERTIFICATE REVOCATION LISTS

This year, Let's Encrypt turned on new infrastructure to support revoking certificates via Certificate Revocation Lists. Despite having been largely supplanted by the Online Certificate Status Protocol (OCSP) for over a decade now, CRLs are gaining new life with recent browser updates.

By collecting and summarizing CRLs for their users, browsers are making reliable revocation of certificates a reality, improving both security and privacy on the Web. Take a closer look at what this new infrastructure does, and why it's important.

A BRIEF HISTORY OF REVOCATION

When a certificate becomes untrustworthy (for instance because its private key was compromised), that certificate must be revoked and that information publicized so that no one relies upon it in the future. However, it's a well-worn adage in the world of the Web Public Key Infrastructure (the Web PKI) that revocation is broken. Over the history of the Web PKI, there have been two primary mechanisms for declaring that a TLS/SSL certificate should no longer be trusted: Certificate Revocation Lists (CRLs) and OCSP. Unfortunately, both have major drawbacks.

CRLs are basically just lists of all of the certificates that a given Certificate Authority (CA) has issued which have been revoked. This means that they're often very large – easily the size of a whole movie. It's inefficient for your browser to download a giant list of revoked certificates just to check if the single certificate for the site you're visiting right now is revoked. These slow downloads and checks made web page loads slow, so OCSP was developed as an alternative.

OCSP is sort of like "what if there were a separate CRL for every single certificate": when you want to check whether a given certificate has been revoked, your browser can check the status for just that one certificate by contacting the CA's OCSP service. But because OCSP infrastructure has to be running constantly and can suffer downtime just like any other web service, most browsers treat getting no response at all as equivalent to getting a "not revoked" response. This means that attackers can prevent you from discovering that a certificate has been revoked simply by blocking all of your requests for OCSP information. To help reduce load on a CA's OCSP services, OCSP responses are valid and can be cached for about a week. But this means that clients don't retrieve updates very frequently, and often continue to trust certificates for a week after they're revoked. And perhaps worst of all: because your browser makes an OCSP request for every website you visit, a malicious (or legally compelled) CA could track your browsing behavior by keeping track of what sites you request OCSP for.

So both of the existing solutions don't really work: CRLs are so inefficient that most browsers don't check them, and OCSP is so unreliable that most browsers don't check it. We need something better.

BROWSER-SUMMARIZED CRLS

One possible solution that has been making headway recently is the idea of proprietary, browser-specific CRLs. Although different browsers are implementing this differently (e.g. Mozilla calls theirs CRLite, and Chrome's are CRLSets), the basic idea is the same.

Rather than having each user's browser download large CRLs when they want to check revocation, the browser vendor downloads the CRLs centrally. They process the CRLs into a smaller format such as a Bloom filter, then push the new compressed object to all of the installed browser instances using pre-existing rapid update mechanisms. Firefox, for example, is pushing updates as quickly as every 6 hours.

This means that browsers can download revocation lists ahead of time, keeping page loads fast and mitigating the worst problems of vanilla CRLs. It keeps revocation checks local, and the pushed updates can take immediate effect without waiting for a potentially days-long OCSP cache to expire, preventing all of the worst problems with OCSP.

Thanks to the promise of these browser-summarized CRLs, both the Apple and Mozilla root programs are requiring that all CAs begin issuing CRLs before October 1st, 2022.

Specifically, they are requiring that CAs begin issuing one or more CRLs which together cover all certificates issued by that CA, and that the list of URLs pointing to those CRLs be disclosed in the Common CA Database (CCADB). This will allow Safari and Firefox to switch to using browser-summarized CRL checking for revocation.

OUR NEW INFRASTRUCTURE

When Let's Encrypt was founded, we made an explicit decision to only support OCSP and not produce CRLs at all. This was because the root program requirements at the time only mandated OCSP, and maintaining both revocation mechanisms would have increased the number of places where a bug could lead to a compliance incident.

When we set out to develop CRL infrastructure, we knew we needed to build for scale, and do so in a way that reflects our emphasis on efficiency and simplicity. Over the last few months we have developed a few new pieces of infrastructure to enable us to publish CRLs in compliance with the upcoming requirements. Each component is lightweight, dedicated to doing a single task and doing it well, and will be able to scale well past our current needs.

Let's Encrypt currently has over 200 million active certificates on any given day. If we had an incident where we needed to revoke every single one of those certificates at the same time, the resulting CRL would be over 8 gigabytes. In order to make things less unwieldy, we will be dividing our CRLs into 128 shards, each topping out at a worst-case maximum of 70 megabytes. We use some carefully constructed math to ensure that – as long as the number of shards doesn't change – all certificates will remain within their same shards when the CRLs are re-issued, so that each shard can be treated as a mini-CRL with a consistent scope.

In line with the same best practices that we follow for our certificate issuance, all of our CRLs will be checked for compliance with RFC 5280 and the Baseline Requirements before they are signed by our issuing intermediates. Although the popular linting library zlint does not yet support linting CRLs, we have written our own collection of checks and hope to upstream them to zlint in the future. These checks will help prevent compliance incidents and ensure a seamless issuance and renewal cycle.

As part of developing these new capabilities, we have also made several improvements to the Go standard library's implementation of CRL generation and parsing. We look forward to contributing more improvements as we and the rest of the Go community work with CRLs more frequently in the future.

Although we will be producing CRLs which cover all certificates that we issue, we will not be including those URLs in the CRL Distribution Point extension of our certificates. For now, as required by the Baseline Requirements, our certificates will continue to include an OCSP URL which can be used by anyone to obtain revocation information for each certificate. Our new CRL URLs will be disclosed only in CCADB, so that the Apple and Mozilla root programs can consume them without exposing them to potentially large download traffic from the rest of the Internet at large.

THE FUTURE OF REVOCATION

There's still a long way to go before revocation in the Web PKI is truly fixed. The privacy concerns around OCSP will only be mitigated once all clients have stopped relying on it, and we still need to develop good ways for non-browser clients to reliably check revocation information.

We look forward to continuing to work with the rest of the Web PKI community to make revocation checking private, reliable, and efficient for everyone.

Building a better Internet, together

THE GLOBAL COMMUNITY BEHIND OUR IMPACT

This year Let's Encrypt was awarded the 2022 Levchin Prize, a major recognition of the impact we've had on real world cryptography—an impact made possible by our global community; a challenge overcome through collaboration and determination.

THE 2022 LEVCHIN PRIZE

The founding of Let's Encrypt has its roots in a group of people recognizing a daunting challenge: billions of people spent an increasingly large portion of their lives online, and they deserved better privacy and security. But in order to achieve that, the group needed to convince websites everywhere to switch to HTTPS. The group wanted to see serious change in TLS adoption in a short timeframe, too. Realizing the solution—Let's Encrypt—was not exactly a eureka moment. Here's what co-founder and ISRG executive director, Josh Aas had to say:

"We thought through a lot of options but in the end we just didn't see any other way than to build what became Let's Encrypt. In hindsight building Let's Encrypt seems like it was a good and rewarding idea, but at the time it was a frustrating conclusion in many ways. It's not an easy solution to commit to.

It meant standing up a new organization, hiring at least a dozen people, understanding a lot of details about how to operate a CA, building some fairly intense technical systems, and setting all of it up to operate for decades.

Many of us wanted to work on this interesting problem for a bit, solve it or at least put a big dent in it, and then move on to other interesting problems. I don't know about you, but I certainly didn't dream about building and operating a CA when I was younger."

Today there are just 11 engineers working on Let's Encrypt. That's not a lot of people for a project serving hundreds of millions of websites in every country on the globe, subject to a fairly intense set of industry rules, audits, and high expectations for security and reliability. The team is preparing to serve as many as 1 billion websites.

SUPPORTED BY A GLOBAL COMMUNITY

It may be the case that Let's Encrypt is a small and nimble team, but so much of our impact is made possible by thousands of people all around the world. Our community remains an important resource for troubleshooting and assisting people as they integrate Let's Encrypt. This year, the Community Forum's average response time to a new post was less than one hour. By the time this year ends, the Community Forum will have exceeded 34 million pageviews!

Our community is just one way Let's Encrypt achieves global impact. We were proud to thank hundreds of people in our orbit for their contributions as part of announcing the Levchin Prize.

The impact of Let's Encrypt over the last ten years has been propelled by people continually contributing their time, energy, and financial resources. We'd like to particularly highlight the following longtime supporters for helping make our work possible.

_az
9peppe
Aanchal Gupta
Aaron Gable
AcademicEDGAR+
Acton Family Giving
ahaw021
Alex Polvi
Alex Zorin
Amir Omidi
Andrew Ayer
Andrew Gabbitas
Andrew Lytvynov
Andrew Marcuse
Andrew Sayler
Arni Johannesson
Audinate
Ayumu Sato
BC Libraries Cooperative
Ben Sykes
Ben Zvan
Benjamin Peskoe
Bjarni Runar Einarsson
Brad Warren
Brian Cunnie
Brian O'Rourke
Bruce Steinberg
Bruce5051
bruncsak
Cadmium
Carl Frederic De Celles
Carrissa Hsieh
Chris Castle
Christine Runnegar
Commercetools
Cory Plastek
Craig Leres
Cullen Jennings
Dalton F.
Dan Fernelius
Dan Jeffery
Dan Tappan
danb35
Daniel Bassa Perez
Daniel Kuebler
Daniel McCarney
Daniel Porteous
David Calavera
David Held
David Nalley
David Pollak
Dean Oakley
Donovan Dikaio
Edwin Bachetti
Eric Anderson
Eric Rescorla
eva2000
Evan Scalzo
EWWW Image Optimizer
Eye Networks
Fabian Wenk
Filippo Valsorda
Finn Odum
Frederic Jacobs
Gareth Bowker
Gavin "Halkeye" Mogan
griffin
Harley Cooper
hikalium
hlandau
Hugues Bruant
Ivan Ristic
J. Alex Halderman
J.C. Jones
Jacob Block
Jacob Helwig
Jacob Hoffman-Andrews
Jacob Whitehill
James O'Gorman
James Renken
Jamie Thingelstad
Jeff Atwood
Jeff Hodges
Jenessa Petersen
Jennifer Granick
Jes Drost Nissen
Jesse Alford
Jesse Wilson
Jillian Karner
JimPas
jmorahan
Joe and Rachel Beda
John Buckley
John Cosgrove
Jonathan Conradt
Josh Aas
Josh Deprez
Joshua Paine
JuergenAuer
Kalle Happonen
Kane York
Karen O'Donoghue
Karl Heinz Marbaise
Katsumi Kishikawa
kelunik
Kevin Bice
Kevin O'Connor
Kiel Chrisofferson
Knut Ahlers
Laban Skollermark
Laura Thomson
Laurent Goujon
Lawrence Chu
leader
Lena Underwood
Liran Cohen
Malcolm Handley
Marc Konvisser
Mary Gardiner
Matt Holt
Matthew Dean
Matthew McPherrin
Matthew Miller
Max Hunter
Maya Kaczorowski
Michael Henretty
MikeMcQ
mnordhoff
Mr. Technique
Neil Schelly
Neilpang
Nick Berry
Niteo
Noah Swartz
Nummer378
Olena Kosheva
orangepizza
Osiris
Pascal Jaillon
Patches
Pauline Middelink
Peter Eckersley
petercooperjr
pfg
Phil Porada
Pietro Cerutti
Preston Locke
rg305
Rich Salz
Richard Barnes
Rip
rmbolger
Roland Shoemaker
Russ Housley
Ryan Dewhurst
Ryan Hurst
Ryan Rhea
sahsanu
Sam Stoelinga
Samantha Frank
Sampsa Hario
Sarah Gran
Sarah Heil
Sarah McClure
schoen
Scott Jann
Scott Munn
serverco
Simon Wisselink
Sinan Taifour
ski192man
Software Effect Enterprises
Sports Reference
Stephanie Wigle
Stephen Ludin
stevenzhu
tdelmas
tialaramex
Tim Geoghegan
tlussnig
Todd Han
Tom Rossi
Tom Van Der Woerdt
Troy Hunt
Vicky Chin
VM (Vicky) Brasseur
Weldon Whipple
WMACCESS Team of CPB Software (Germany) GmbH

The certificate system is a great example of an Internet infrastructure that puts to use real-world trust relationships towards a functioning technical trust "anchor." Billions of people access the Internet with less censorship and surveillance because Let's Encrypt hastened the adoption of web security measures by making certificates easy to obtain."

MALLORY KNODEL
CHIEF TECHNOLOGY OFFICER
CENTER FOR DEMOCRACY & TECHNOLOGY

Shifting the privacy paradigm

A TECTONIC SHIFT FOR PRIVACY

Divvi Up will help app makers, and the platforms enabling them, go beyond the promises of a privacy policy to provide cryptographic guarantees of privacy when user information is collected and handled. It's a tectonic shift, but one that's possible.

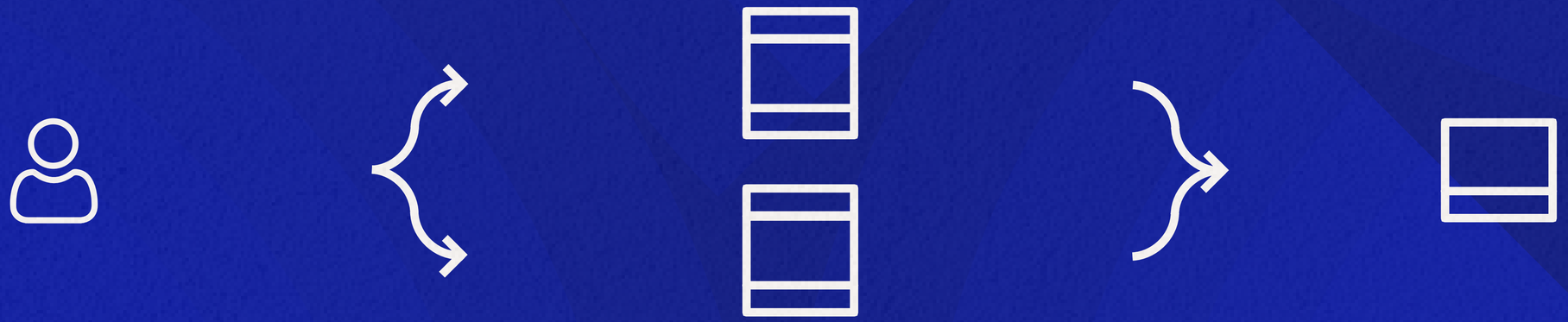
Divvi Up

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 recombines them into a privacy-preserving aggregate.



A USER-GENERATED VALUE

DIVIDE THE VALUE

TWO, NON-COLLUDING SERVERS

COMBINE AGGREGATES

ANONYMIZED INSIGHT

BEYOND THE PRIVACY POLICY

Today, any app creator who seeks to gain access to an audience has two main platforms to do so: the Apple App Store and the Google Play Store. Both of these platforms set requirements for developers to meet before their app can be listed—a content rating, setting pricing, meeting various technical requirements, and publishing a privacy policy.

Some of these requirements are technical checkboxes that are reviewed by Google and Apple. For example, all Android apps are required to be digitally signed before they can be installed on a user's device. Failing to meet these technical requirements results in an app not being listed. However other requirements are much simpler and subjective, like setting pricing and a privacy policy. Importantly, the privacy policy requirement is simply, "Enter the URL hosting the privacy policy online."

Looking at the top ten downloaded applications in countries like Belarus, Mexico, and Bahrain, you might expect to see well-known apps like WhatsApp, YouTube, and Facebook. You'd expect these apps to have well-established privacy policies and, of course, they do. However, what you'll also find are apps like Poppy Horror: Chapter One, and Бабл Квас which in early 2022 were among the top five downloaded apps in these countries.

Inspecting the privacy policies of Poppy Horror and Бабл Квас (whose policy is nothing more than a Google Doc), it is clear that users' privacy is far from top of mind. Despite this, these apps are widely popular.

These are just two examples that illustrate the larger problem: developing a policy for how an app impacts user privacy is practically unenforceable. What's more, users have no assurance of how an app might actually use their information, regardless of what is promised in the privacy policy.

Apple and Google know this is a problem. They're already laying the groundwork to address it. In 2021, both companies announced a change to their platforms requiring app developers to be transparent about the data they collect.

This isn't the first time Apple and Google have updated their policies for app store requirements. Prior to 2016, iOS apps weren't required to use HTTPS. One fundamental reason this was the case is that it

wasn’t practical for Apple to require this change. Let’s Encrypt, in large part, made it practical for Apple to require TLS for application network connections.

ISRG provided an easy way for anyone to use HTTPS; Apple and Google made app developers' adoption of TLS non-negotiable. These two changes together created more security and privacy for everyone using these platforms around the world. It made every app that’s ever been listed since then more secure.

We have a similar aim for Divvi Up. Requiring anything more than a url with a privacy policy wasn’t feasible a few years ago. Today, requiring explicit privacy disclosures by developers is happening, but that is still not enough to improve user privacy. When Divvi Up is widely available and easy to use, as we intend to do, technologically guaranteeing peoples’ privacy will be feasible.

Fundamentally, we don’t need Apple and Google to enforce privacy. We only need to build a technology that is so easy to use, for anyone around the world, that the alternative of not using a privacy-preserving metrics service like Divvi Up becomes as unthinkable as not using TLS for HTTP today.

> **The idea that you can put sensitive data into a system and be able to get an accurate summary of that data without people having access to the specifics is very useful. For example, if independent review boards get wind of this, it could revolutionize science. Scientists could get exact summaries of the information without people having to give up their exact data."**

RICHARD BARNES
CHIEF SECURITY ARCHITECT FOR COLLABORATION
DISTINGUISHED ENGINEER
CISCO

Setting a new standard

OUR WORK WITH DIVVI UP AT THE IETF

ISRG has a well-established track record of building technology that will benefit everyone using the Internet. That aim wouldn't be possible without taking a collaborative approach, particularly within the Internet Engineering Task Force (IETF) and with other key partners.

We intend to resolve much of the tension between wanting to know information about a population of people and needing to collect information about individuals that might compromise their privacy. While the IETF's Distributed Aggregation Protocol (DAP) specification is still under active development, we have developed a DAP client, collector, and aggregator called Janus (named after the Roman deity of duality!). We then launched pilots aggregating data with our partner organizations.

These pilots have served to prove out the privacy guarantees and other properties of the system. Various metric types based on the Prio aggregation scheme by Dan Boneh and Henry Corrigan-Gibbs have been collected & verified as correctly aggregated, showing that numerical metrics can be aggregated in a privacy-preserving way. While productionization and scaling work is ongoing, the initial performance properties of the system are promising and in-line with the theoretical expectations for the underlying aggregation schemes.

"While productionization and scaling work is ongoing, the initial performance properties of the system are promising"

We are excited to continue developing DAP & Janus into the future. We will soon begin testing with the Poplar aggregation scheme currently undergoing standardization, which will allow common reported values to be discovered without impinging on the privacy of individual reports. We will also productionize and scale Janus; we will soon begin a production-quality pilot aggregating data with privacy requirements.

On track towards a more private future

WHERE WE ARE TODAY WITH DIVVI UP

The team has made tremendous progress on further developing Divvi Up and the DAP standard. Here's a closer look at what we've done, where we are, and where we're going.

ISRG continued to serve as one of the data processors in the Prio-based privacy-preserving metrics system used by Apple and Google's Exposure Notifications Express (ENX), known as Exposure Notification Private Analytics (ENPA). This year has seen the system expand to several new US & international localities, providing reliable and accurate data about the spread of COVID to health experts and officials in these communities without impinging on individuals' privacy. ISRG has been participating in this collaboration since 2020 and the system has processed over 40B metrics with consistency and reliability.

The design and implementation of ENPA had a great deal of influence on the design of the later Distributed Aggregation Protocol (DAP). The core of the aggregation design in DAP is very similar to that of ENPA's. The time-windowing and aggregation design allows for aggregation & collection to happen concurrently, which is critical to reach the performance & scalability goals of a design such as DAP.

ENPA's implementation has also affected the design & implementation of Janus, ISRG's DAP implementation. The ENPA deployment strategy tightly coupled the implementation code with the deployment configuration, to the point that all organizations deploying ENPA effectively deployed the same configuration. This coupling allowed ENPA to be deployed more quickly, but drastically increased the cost of deploying later changes to the system. Janus was careful to take a deployment strategy which loosely-coupled the implementation code with the deployment configuration; this has made Janus much easier to deploy. We are already seeing the benefits of this: at least one partner organization was able to deploy Janus with no assistance whatsoever from the ISRG.

THE FUNDERS BEHIND DIVVI UP

ISRG has raised more than $1.5M for Divvi Up, led by the Open Tech Fund and joined by the Ford Foundation, the Robert Wood Johnson Foundation, the Internet Society Foundation, Acton Family Giving, Meta, and Google.

This funding will help ISRG continue to develop Divvi Up, a project focused on fundamentally improving peoples' privacy when they engage with apps, websites, or other technology collecting their data.

Divvi Up provides an opportunity to dramatically improve user privacy. It's because of that potential these leading funders have stepped up to help make this work possible. Divvi Up got its start as part of a massive undertaking to use advanced technology to help mitigate the spread of COVID-19. We were proud to be part of that effort. Now, we're expanding Divvi Up to serve a much broader range of use cases.

The Open Tech Fund (OTF) is providing $845,444 to support the development of Divvi Up and the work to standardize the underlying protocol with the IETF. "OTF is pleased to see ISRG advance user privacy via Divvi Up, particularly for people in repressive Internet environments," OTF President, Laura Cunningham, said. "Ensuring everyone around the world can use the Internet for their benefit is critical—ensuring their security and privacy is paramount. ISRG and its projects are helping lead the way to protecting security and privacy for all users of the Internet around the world."

The Ford Foundation and Robert Wood Johnson Foundation both provided $40,000 to support Divvi Up.

Paul Tarini, senior program officer at RWJF commented, "Personal health data is some of the most sensitive information and Divvi Up is designed to protect the privacy of that information. Apps and other technologies are becoming an integral part of how we deliver health and health care services, yet many people are concerned about the privacy of the data they provide," Paul said. "We hope Divvi Up works for a broad range of organizations so that as many people as possible can benefit from health technology while preserving their own privacy."

"We want to see privacy preserving metrics used *everywhere*, by default, not just for metrics that are considered to be sensitive. Sometimes metrics can reveal personal information even if they don't appear to be sensitive."

WINDOW SNYDER
FOUNDER & CEO
THISTLE TECHNOLOGIES

Bringing memory safety to the fore

MOVING TOWARDS A MEMORY SAFE INTERNET

Launched in 2020, Prossimo continues to lead the world toward a future where the Internet's critical software infrastructure uses memory safe code. This year, we partnered with maintainters to support memory safety initiatives affecting the most critical components of the Internet ecosystem.

PROSSIMO

FOR MEMORY SAFETY

Rust in the kernel

A CLOSER LOOK AT OUR ROLE IN THIS WORK

The Prossimo project launched our Linux kernel initiative knowing that the Internet would be more secure if it was possible to write Linux kernel modules in a memory safe language. Now that's becoming a reality. Support for using Rust in the Linux Kernel was merged in early October of this year by Linus Torvalds...

The inclusion of Rust is an exciting step to improving the security of the Linux kernel. At Futurewei, we are glad to contribute to this effort's momentum by supporting it through ISRG's Prossimo."

SID ASKARY
SENIOR MANAGER OF OPEN SOURCE
FUTUREWEI

Rust is a memory safe programming language, meaning code written in Rust does not suffer from things like buffer overflows, use-after-free, and other memory management vulnerabilities that plague software written in unsafe languages like C and C++. Being able to use Rust in the Linux kernel is an incredible milestone on the road to a more secure future for the Internet and everything else that depends heavily on Linux.

This milestone is thanks in great part to incredible work done by Rust for Linux developer Miguel Ojeda, who we've worked with since 2021 to help make it possible. We'll continue our work with Miguel Ojeda into 2023 and will also be working with Gary Guo, another Rust for Linux contributor, on improving the Rust compiler's support for features needed in the kernel.

Support for using Rust in the Linux kernel is just the beginning. In order for progress to continue, this new capability needs to be used to develop and merge safer device drivers and possibly other kernel components written in Rust. To this end, we are identifying Rust drivers that would benefit from investment. One of the most promising is an NVMe driver that has shown impressive initial performance metrics. We're also encouraging companies that maintain drivers for their hardware to experiment with moving drivers to Rust.

We're incredibly proud to have been a part of this significant advancement, one that required years of hard work. We look forward to continuing our work to help make the Linux kernel more memory safe and in turn the Web more secure for everyone, everywhere.

Our critical focus

BRINGING MEMORY SAFETY TO FOUR INITIATIVES

Building on our work from 2020 and 2021, this year ISRG began or continued work on bringing memory safe code to Internet-critical software. From rustls to NTP to DNS and tooling, we're taking the steps to keep the Web's most critical software secure.

RUSTLS

The problem: OpenSSL is a TLS library that is used by a majority of devices connected to the Internet. Unfortunately, OpenSSL is written in the programming language C, which is not memory safe, and it has a long history of memory safety issues, including two high severity vulnerabilities that were patched this year.

The progress: It's highly unlikely the OpenSSL project will move away from C, so we identified a memory safe alternative to the Internet's critical software infrastructure: Rustls. Rustls is a high-quality TLS implementation written in the memory safe programming language Rust and is an excellent alternative to OpenSSL for many use cases. ISRG believes Rustls represents the future of TLS implementation on the Internet.

We worked with Dirkjan Ochtman, an experienced Rust developer and Rustls contributor, to make a number of improvements to the Rustls library. Our own engineer, Jacob Hoffman-Andrews, developed a C API for Rustls that existing C-based projects can use to make their TLS implementation memory safe. We're continuing to raise funds for further improvements to Rustls.

NETWORK TIME PROTOCOL (NTP)

The problem: Network Time Protocol (NTP) is how the Internet keeps track of time. It synchronizes time between devices connected to a network making sure events are ordered correctly. As one of the oldest Internet protocols, the Internet and its billions of devices depend on NTP every day.

Unfortunately, the most popular NTP implementations today are written in the programming language C, which is not memory safe. This vulnerability could be used by attackers to, for example, adjust the system time such that an outdated TLS certificate is seen as valid. The primary goal for this project has been to provide an alternative implementation of NTP that is secure and reliable.

The progress: We partnered with the team at Tweede golf to develop an NTP client and server in the memory safe language Rust; it's called NTPd-rs. Next we aim to support the adoption of Network Time Security (NTS) support which will add features to offer even more security when using NTPd-rs.

DNS

The problem: Known as the phonebook of the Internet, DNS translates domain names into IP addresses. Nearly all clients and servers depend on making frequent DNS lookups, making it as critical as Internet infrastructure gets.

While there are many DNS implementations out there, including some memory safe ones, there are no open source, high performance, memory safe, fully recursive DNS resolvers. Until that exists, many DNS operators will continue to deploy DNS software written in languages that are not memory safe, putting critical Internet infrastructure at risk.

The progress: We're working with Benjamin Fry on his memory safe DNS implementation in the Rust programming language. This implementation has become a useful piece of software in production environments for stub resolution, simple authority use cases, and cache warming for DNS providers.

Let's Encrypt will be amongst the first to deploy this memory safe implementation, proving its performance at scale by making thousands of recursive requests per second. In turn, our Let's Encrypt infrastructure will be more memory safe.

TOOLS

The problem: In order to move critical software infrastructure to memory safe code there needs to be as little friction as possible. Great tools make the memory safe choice an easier one for engineering teams to make.

The progress: We partnered with Rémy Rakic, a member of the Rust compiler team, to improve Rust compile times. We also partnered with Ferrous Systems to make various improvements to the bindgen tool. We plan to continue our work with both Rémy Rakic and Ferrous Systems into 2023.

"Memory safety issues are responsible for a huge, huge percentage of all reported vulnerabilities, and this is in critical applications like operating systems, mobile phones, and infrastructure."

DAN LORENC
CEO
CHAINGUARD

Small makes mighty

PEOPLE, FUNDERS, & FINANCIALS

2023 marks the tenth anniversary of ISRG. Looking ahead to that milestone is a good opportunity to begin looking back at the people, funders, and leadership who've helped us get there.

ISRG

Internet Security Research Group

The road ahead

LETTER FROM ISRG BOARD CHAIR, CHRISTINE RUNNEGAR

ISRG has come a long way since its start in 2013, nearly ten years ago.

ISRG is widely regarded as a role model for operating public-benefit Internet infrastructure. First, by running and maintaining the open, free, and automated certificate authority, Let's Encrypt, and subsequently, for its leadership in the Prossimo and Divvi Up projects. ISRG has shown that public-benefit infrastructure can be both successful and sustainable.

ISRG would not be where it is today if it were not for the tremendous support received from

partners, sponsors, donors, funders, users, the open source community, and the many individuals who devote their time and resources to helping us realize our vision of a more secure and privacy-respecting Internet. Thank you!

With your contributions, ISRG provides free digital certificates reliably to millions of websites, ensuring that users have a more secure and privacy-respecting experience on the Internet. We are supporting community efforts to replace core Internet infrastructure software with memory safe code, which will help to eliminate common security vulnerabilities on the Internet. We are also leading a major shift in the way online application metrics will be analyzed towards secure multiparty computation to better preserve users' privacy.

We want to thank Josh Aas, our Executive Director, who has been instrumental in making ISRG the highly efficient and sustainable nonprofit organization it is today. Under his leadership, ISRG has built an impressive team and fine-tuned its operations to effectively use your financial support to achieve reliable services at scale.

We also wish to thank the Linux Foundation, which provided ISRG with an initial home and helped ISRG by taking care of internal operations, such as human resources and accounting, so that ISRG could concentrate on delivering a trusted and reliable public-benefit service to everyone during its first years. Starting next year, we will be joining the Linux Foundation in a new capacity, as a nonprofit Member.

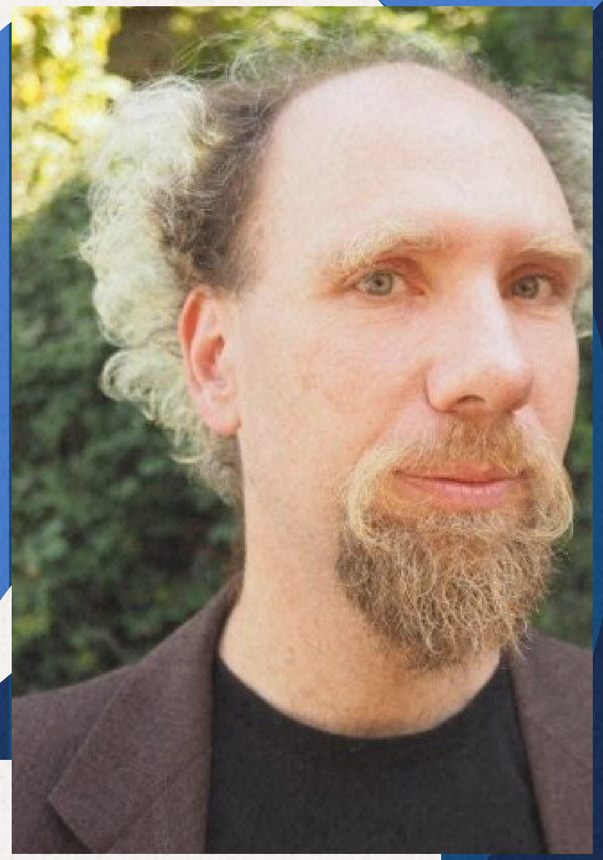
2023 will be an exciting time for ISRG as an organization.

Not only will we be embarking on our 10th anniversary, but, for the first time, we will also be handling all aspects of our internal operations in-house. This will streamline ISRG's internal operations, create more agility, and allow us to benefit fully from the ideas and expertise of our wonderful staff. They are the reason why Let's Encrypt can provide TLS certificates to more than 300 million websites worldwide and ISRG can take on new innovative work to improve Internet security and privacy.

Building organizational capacity is not something to do overnight. ISRG has been preparing for this moment over the last two years, figuring out how to handle the complexity of managing additional projects with different financial and operational requirements, enhancing our fundraising capacity, and ensuring we are using our staff resources most effectively.

We are conscious that the global economic outlook for 2023 is uncertain, at best. We have already seen the effects of inflation on ISRG's operating costs, and delays in hardware availability across the tech industry. However, thanks in-large-part to strong support from our global community, ISRG is well-positioned to mitigate some of the uncertainty by rearchitecting services to use existing resources more efficiently, and having already made extensive upgrades to our infrastructure to enhance the stability and resilience of Let's Encrypt.

We are grateful for your ongoing financial support. We are looking forward to another year contributing to an even more secure and privacy-respecting Internet.



Remembering Peter Eckersley

ENERGY, OPTIMISM, KINDNESS, AND THE PURSUIT OF KNOWLEDGE

Peter Eckersley, a Let's Encrypt co-founder, passed away unexpectedly on September 2nd from complications of cancer treatment. As an incredibly kind, bright, and energetic person, he was a beloved member of the community of people working to make the Internet a better place. Peter played an important role in the founding of Let's Encrypt and his loss is felt deeply by many in our organization and community.

Peter met Alex Halderman at the RSA Conference in 2012 and the two of them started to make plans for technology to automate the process of acquiring HTTPS certificates. This work included early designs for what would become the ACME protocol. Peter and Alex later teamed up with a parallel effort by Josh Aas and Eric Rescorla at Mozilla, and the four of them worked together to create a new automated public benefit CA. The result was Let's Encrypt, which began service in 2015.

Peter also led the development of the initial ACME client, which would eventually become Certbot. In a reflection of Peter's vision for making the Internet secure by default, Certbot aims to fully automate HTTPS deployment, rather than simply procure a certificate. Today, Certbot is among the most popular ACME clients, and it is developed and maintained by Peter's former team at the Electronic Frontier Foundation (EFF).

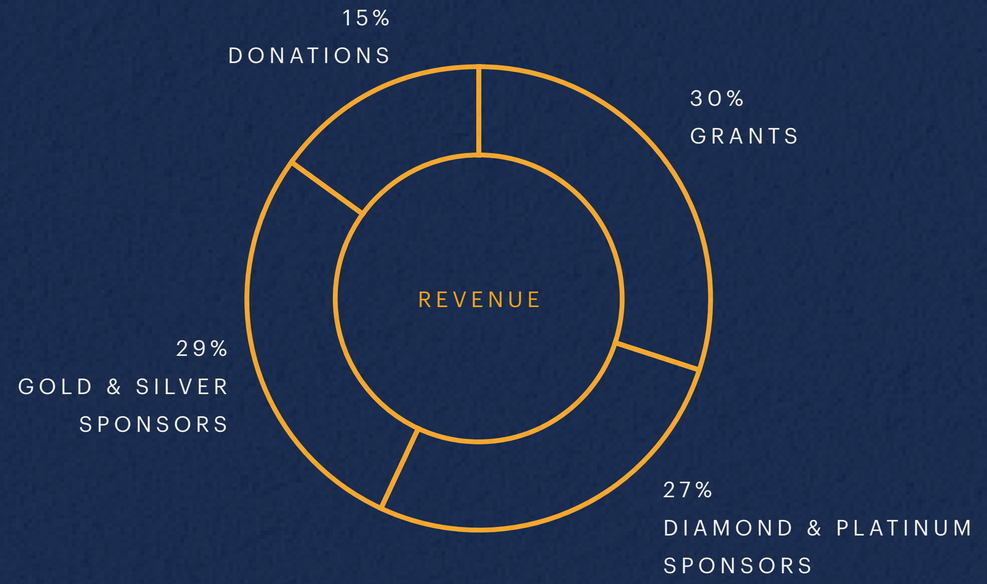
Peter was a member of our Board of Directors for several years. We greatly valued his contributions as a Director, but one of the memories from that time that makes us smile the most is Peter's habit of showing up to board meetings with a messenger bag over his shoulder, helmet hair, and rosy cheeks from arriving by bike.

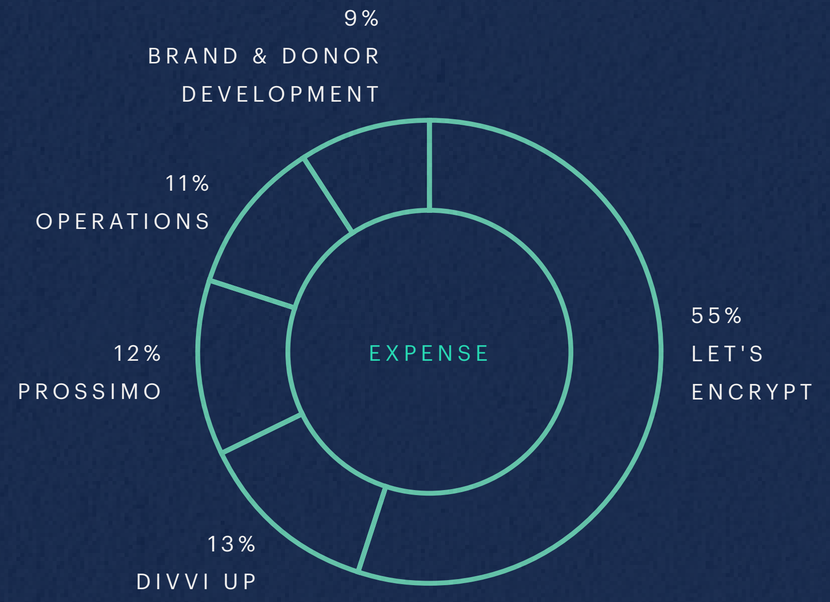
Making change at scale on the Internet is not easy. One way to get it done is to be both a dreamer and someone who possesses the deep technical knowledge necessary to bring dreams to reality. Peter was one of those people, and we're grateful to have been able to work with him.

We hope to honor Peter's life by letting the qualities we admired so much in him - his energy, optimism, kindness, and pursuit of knowledge - inspire our efforts going forward.

Financials

Today ISRG supports a staff of more than twenty, runs three projects to advance its mission, and is in strong financial position as it heads into 2023.





> **With our security-oriented mindset, we proudly support Let's Encrypt and its work with encryption to make the Web more secure for all."**

ALON MUCHNICK
R&D MANAGER - PREMIUM PRODUCTS
WIX

Funders

Nearly one hundred sponsors and funders from more than twenty countries around the world supported us in 2022.

From one-employee shops to thousand-employee companies, we are proud to have support from these organizations who prioritize the importance of investing in a more secure and privacy-respecting Web.

> **We have supported Let's Encrypt since the very beginning. It is very valuable and important that nowadays any website can be equipped with an SSL certificate free of charge."**

MARKUS GEBERT
CO-FOUNDER & CEO
HOSTPOINT

Board & Staff

2022 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

ISRG STAFF

AARON | SOFTWARE ENGINEER
ANDREW | SOFTWARE ENGINEER
BRANDON | SENIOR SOFTWARE ENGINEER
CARRISSA | PEOPLE MANAGER
DAN | SENIOR DEVELOPMENT OFFICER
DAVID | SOFTWARE ENGINEER
FINN | BRAND & DONOR DEVELOPMENT COORDINATOR
JACOB | SOFTWARE ENGINEER
JAMES | SITE RELIABILITY ENGINEER
J.C. | SITE RELIABILITY ENGINEER
JOSH | EXECUTIVE DIRECTOR
KIEL | SITE RELIABILITY ENGINEER
LENA | SITE RELIABILITY ENGINEER
MATTHEW | SITE RELIABILITY ENGINEER
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 ASSOCIATE
TIM | SITE RELIABILITY ENGINEER

Let's build a better Internet, together.

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

OUR THANKS TO THESE INDIVIDUAL DONORS

This year we received thousands of donations from countries all around the world.
Our thanks to these donors who included a name for recognition for their support.

100 PROCENT BAND
AJ Jordan
Aldo Viruez
alejandro arteaga
Alphéa.net
Alun Stokes
Amar
Anatolii Kravchuk
Andrzej Pauli
Ann and Duncan Sterling
ANNOP
CHAWALITSITTHIKUN
Antonios Chariton
apanymantel.com
Artan Sinani
Arunesh
aspectra AG
Ayat
Badassops LLC
Bahaa Monder
Bearium Networks LLC
BeAuTfLi Life
Bertrand Might
BlackCrystal Oú
Bob
BRACE GmbH
Brian Cunnie
Chris Wilson
Christi Scarborough
Clearbold, LLC
Clint Olsen
COMPANIA FITNESS
Cristian Mihalache
Crown Consult
Curium Technologies
Dan Manners
Daniele Verducci
Dianne Skoll
do.de | Domain-Offensive
donation for two domain
names
dvsEVE EEW
Elie El Daher
Epsitec SA
Eric Fritz
Eric Pannetier
Erick Siordia Nagaya
Evgeny Cherkashin
felipe ignacio noriega
Francesco Belacca
Francisco Gonzalez
Gary Gapinski
George Byrne
Gregory Werbin
Hodfords
Honest Antonis CA
Infinum d.o.o.
inGenerator Ltd
Isaac Holmes
Ivan Monnier
김한수
Jörg Strohmeier
JEN
Jerónimo MORALA
REYERO
Joachim Vosberg
Kevin Kaland, WizOne
Solutions
Khresterion SAS (Paris)
Kuick LLC
Kyva Veenk
Legion Technologies Inc.
Leo Macke
Marc DS
Marshall D
masaki goto
Mathias
matt sossi
Michael Januschewsky
midrange.com
Moval Agroingenieria
MrCall AI
Nate S.
nicosch
no
Nordine VALLAS
Pedro Cunat Medina
Performance Logic
Peter Ackermann
Peter Eckersley
Phoebe Dobson
QBIST Inc.
quickytools
Rüdiger Cieslok
Red Madrone Solutions
René Rehag
resume-template.online
RICARDO SOARES DE
OLIVEIRA
rictic
Rober Pankrath
Roger Goudarzi & Nicola
Downes
Ryan Cragun
Salvatore Denaro
Samer Attallah Mhana
Servicios KG Online S.L.
Showit, Inc.
Snap Surveys Ltd
soebes
SrGMC
Stefan Foulis
Thomas O'Connor
Tim
Timofey Bugaevsky
Tobias Ribizel
Tom Carden
Torutek
Tracy Di Marco White &
Jason White
Trident Honda
Turritopsis Dohrnii Teo En
Ming
Vadim Glebov
Valerie Bock
VINN
Vu Duy Tu
Watcharasak Sudla
Webstel Computer
Systems
wehavestock
Wellington Torrejais da
Silva
Widda Alata
Zero3

Donors are listed alphabetically and recognized exactly as submitted. Only donors who, at the time of donating, provided a recognition name are listed.