OpenSSL Foundation

February 1, 2026

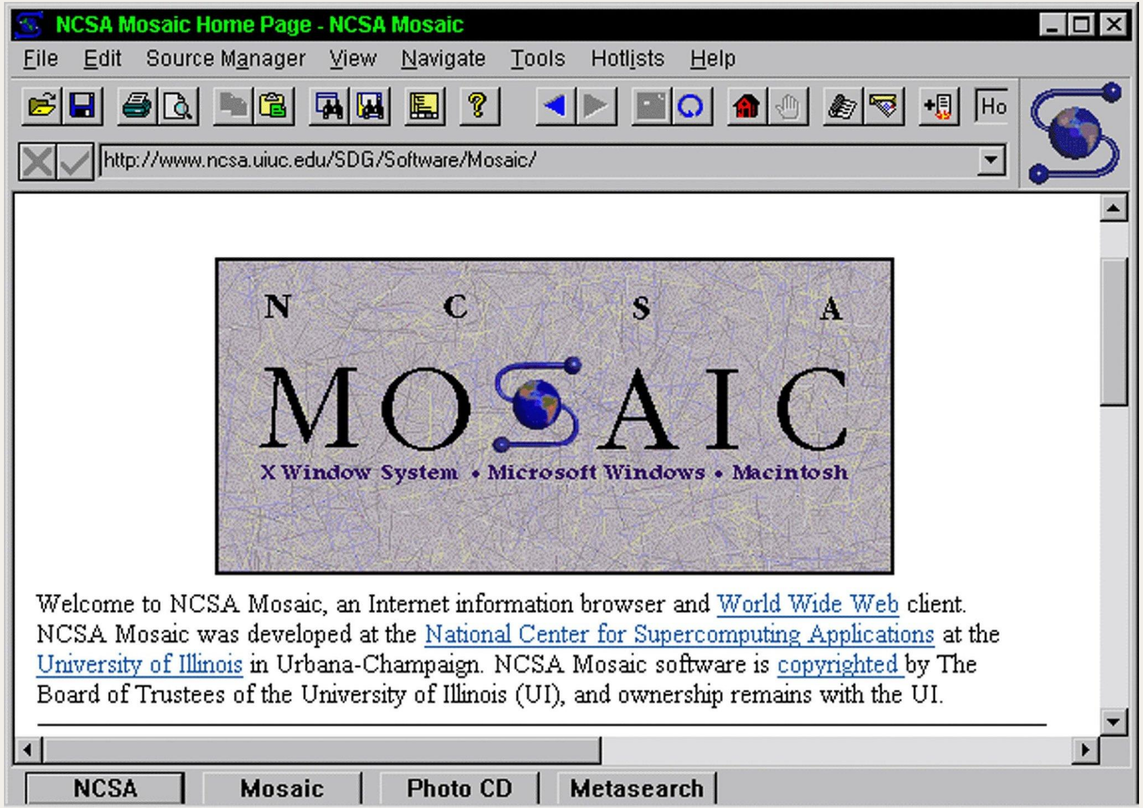
How the OpenSSL community was built on Heartbleed

Jon Ericson
Communities Manager
OpenSSL Foundation

The OpenSSL Mission

We believe **everyone** should have access to **security** and **privacy** tools, whoever they are, **wherever** they are or whatever their personal beliefs are, as a **fundamental human right**.

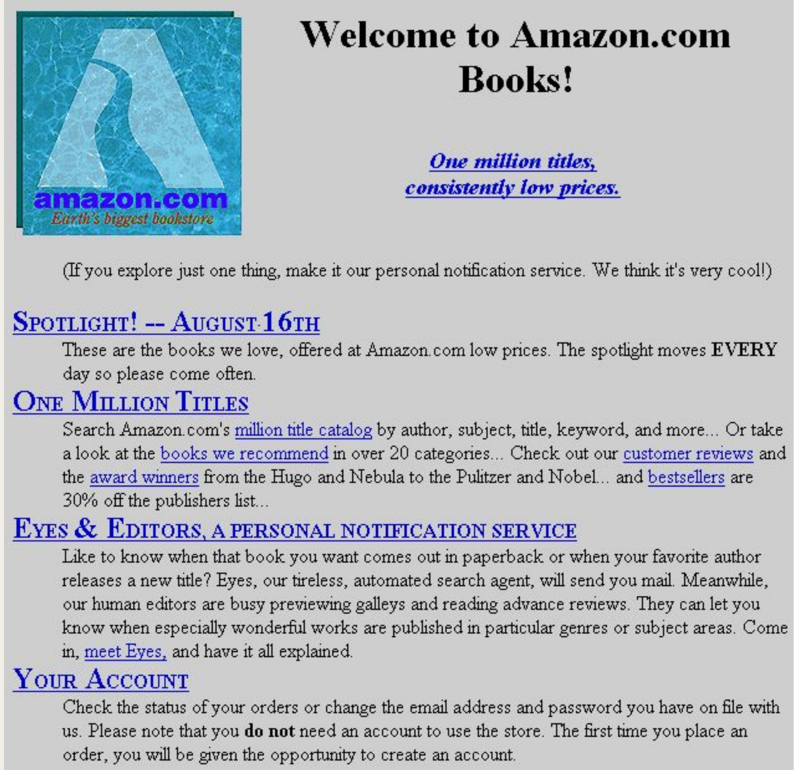
World Wide Web (not secure by default)



NCSA Mosaic Home Page - NCSA Mosaic
File Edit Source Manager View Navigate Tools Hotlists Help
Ho
http://www.ncsa.uiuc.edu/SDG/Software/Mosaic/
N C S A
MOSAIC
X Window System • Microsoft Windows • Macintosh
NCSA
Mosaic
Photo CD
Metasearch

Welcome to NCSA Mosaic, an Internet information browser and World Wide Web client. NCSA Mosaic was developed at the National Center for Supercomputing Applications at the University of Illinois in Urbana-Champaign. NCSA Mosaic software is copyrighted by The Board of Trustees of the University of Illinois (UI), and ownership remains with the UI.

So how can it be used to sell stuff?



Welcome to Amazon.com Books!

One million titles, consistently low prices.

(If you explore just one thing, make it our personal notification service. We think it's very cool!)

Spotlight! -- August 16th

These are the books we love, offered at Amazon.com low prices. The spotlight moves **EVERY** day so please come often.

One Million Titles

Search Amazon.com's million title catalog by author, subject, title, keyword, and more... Or take a look at the books we recommend in over 20 categories... Check out our customer reviews and the award winners from the Hugo and Nebula to the Pulitzer and Nobel... and bestsellers are 30% off the publishers list...

Eyes & Editors, a personal notification service

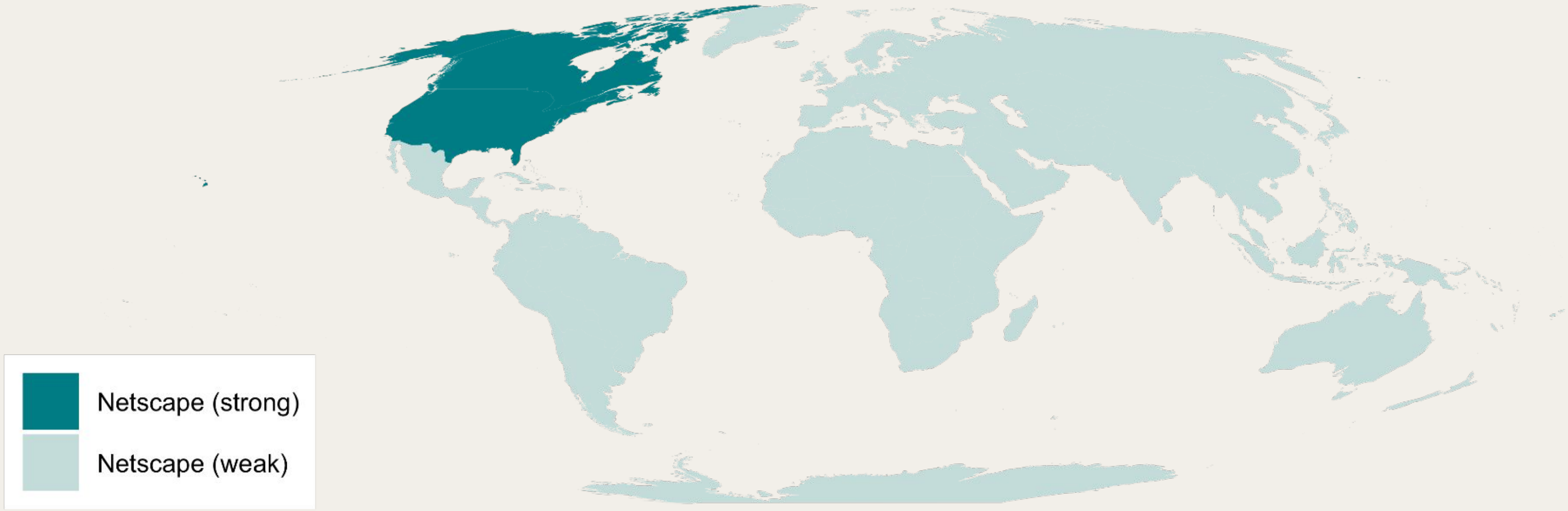
Like to know when that book you want comes out in paperback or when your favorite author releases a new title? Eyes, our tireless, automated search agent, will send you mail. Meanwhile, our human editors are busy previewing galleys and reading advance reviews. They can let you know when especially wonderful works are published in particular genres or subject areas. Come in, meet Eyes, and have it all explained.

Your Account

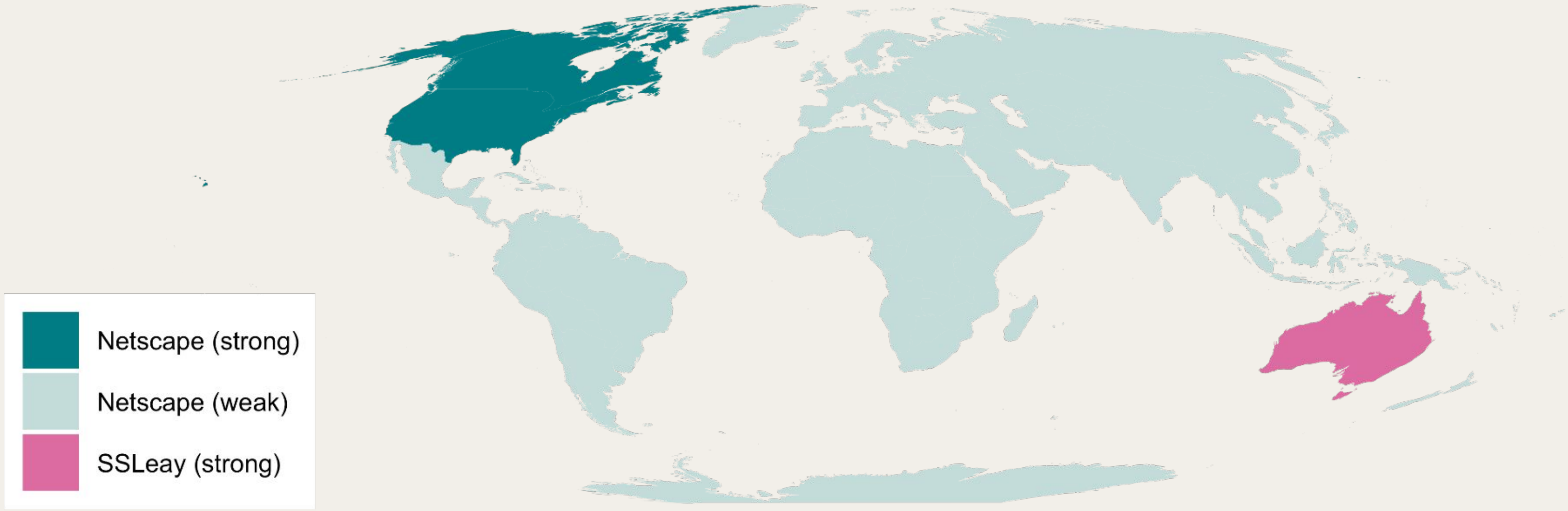
Check the status of your orders or change the email address and password you have on file with us. Please note that you **do not** need an account to use the store. The first time you place an order, you will be given the opportunity to create an account.

Netscape SSL to the rescue

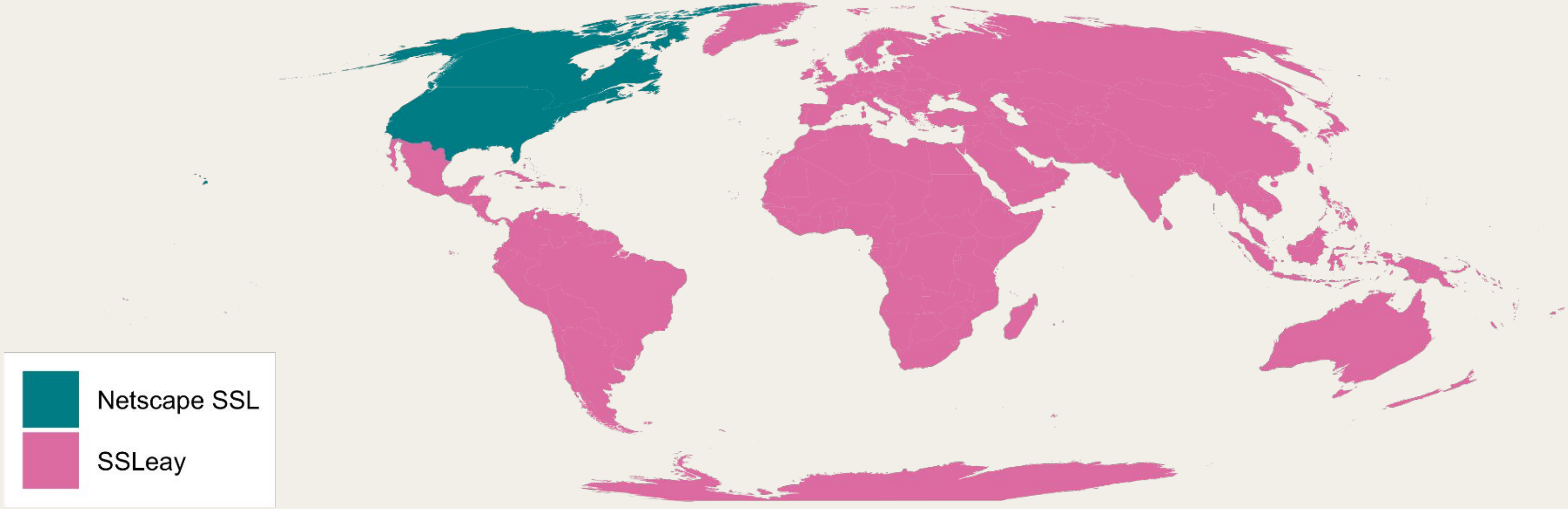
1995: Netscape’s strong encryption (for some)



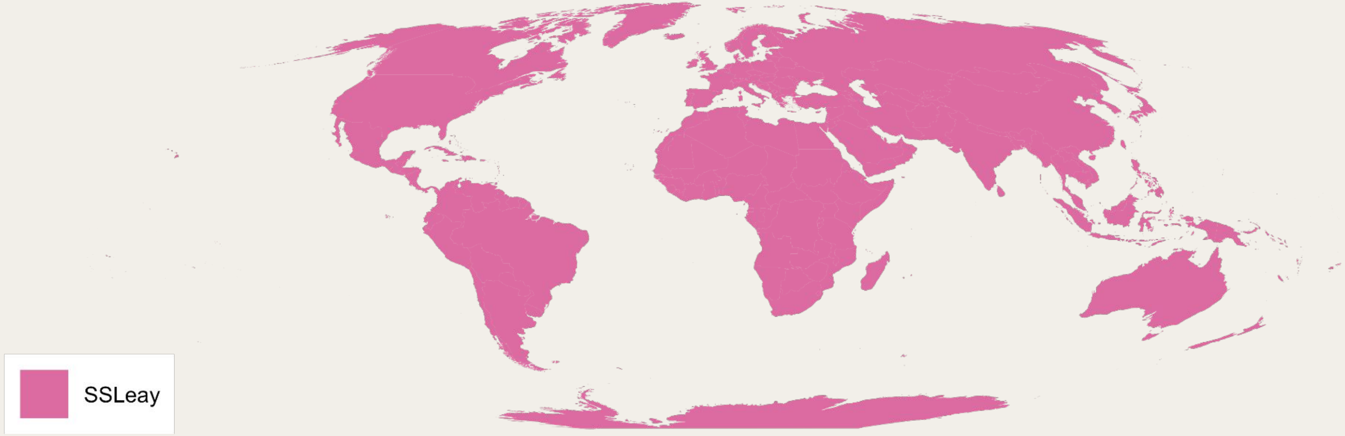
1995: Scratch that itch!



The Australia Strategy



SSLeay empowered other open source projects



Still a lot of Netscape SSL, however.

And then the SSLeay founders left to join RSA.

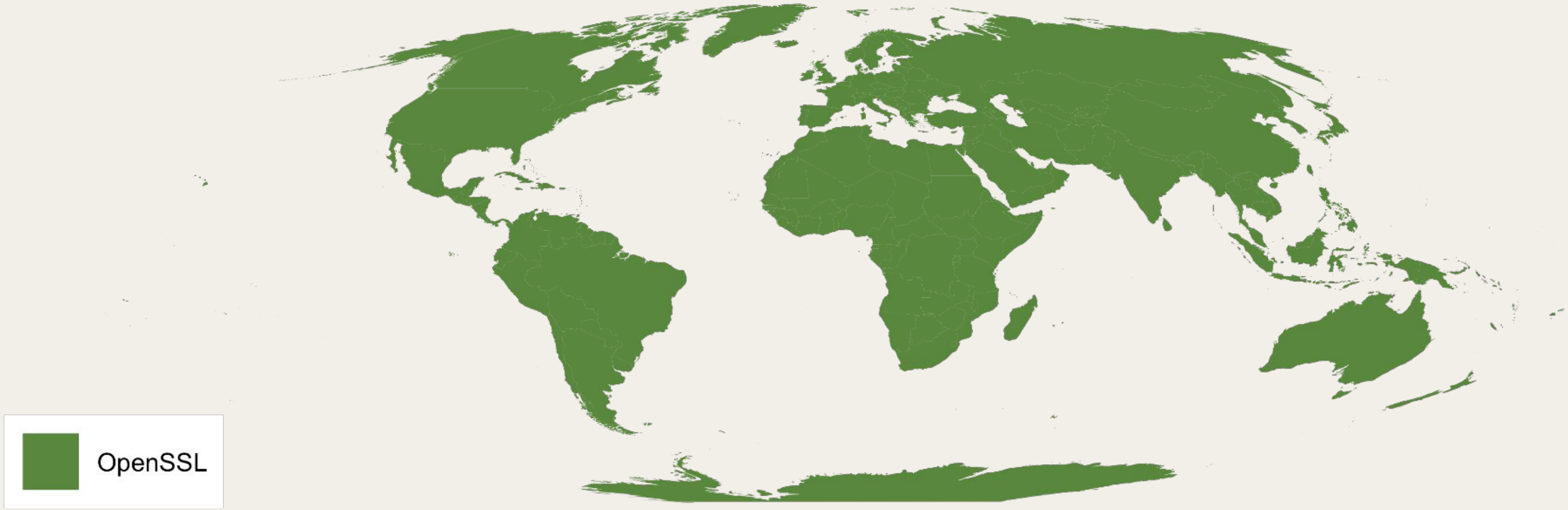
List: ssl-users
Subject: [ssl-users] ANNOUNCE: OpenSSL (Take 2)
From: Ben Laurie <ben () algroup ! co ! uk>
Date: 1999-01-06 22:03:02

```
  ___                  ____ ____  _
 / _ \ _ __  ___ _ __ / ___/ ___|| |     OpenSSL
| | | | '_ \/ _ \ '_ \\___ \___ \| |     The Open Source toolkit for SSL/TLS
| |_| | |_) | __/ | | |___) |__) | |___  http://www.openssl.org/
 \___/| .__/\___|_| |_|____/____/|_____|
_____ |_| __________________________________________________________________
```

The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, fully featured, and Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols with full-strength cryptography world-wide. The project is managed by a worldwide community of volunteers that use the Internet to communicate, plan, and develop the OpenSSL tookit and its related documentation.

OpenSSL is based on the excellent SSLeay library developed by Eric A. Young and Tim J. Hudson. The OpenSSL toolkit is licensed under an Apache-style licence, which basically means that you are free to get and use it for commercial and non-commercial purposes subject to some simple license conditions.

1999: OpenSSL everywhere doing everything



2014: Heartbleed put OpenSSL in the news

"All the News That's Fit to Print"

The New York Times

Late Edition

Today, sunshine and clouds, windy, a bit cooler, high 58. **Tonight,** clear, diminishing wind, low 40. **Tomorrow,** mostly sunny, breezy, mild, high 62. Weather map, Page A14.

VOL. CLXIII . . . No. 56,466 + © 2014 The New York Times NEW YORK, WEDNESDAY, APRIL 9, 2014 $2.50

U.S. and NATO Warn Kremlin Not to Meddle in Ukraine

Secretary of State John Kerry blamed Moscow for unrest as pro-Russia protesters built barricades Tuesday in Donetsk. Page A4.

Sliver of Medicare Doctors Get Big Share of Payouts

Huge Trove of Health Data Is Disclosed — $21 Million for One Physician in '12

By REED ABELSON and SARAH COHEN

Banks Ordered To Add Capital To Limit Risks

By PETER EAVIS

Tearful Drama as Pistorius Says He Panicked

Sheds Prosthetics in Telling How He Shot Girlfriend

By SARAH LYALL

UConn Wins It All

Connecticut's women matched the men and won the N.C.A.A. basketball title, defeating Notre Dame, 79-58. Above, UConn's center, Stefanie Dolson, battling Taya Reimer. Page B12.

WHITE HOUSE MEMO

What Would Johnson Do?

By PETER BAKER

Best, Brightest and Rejected: Elite Colleges Turn Away Up to 95%

By RICHARD PÉREZ-PEÑA

Mining Women's Votes

BUSINESS DAY B1-11

Automakers' Inroads in China

Global auto manufacturers like Ford Motor are steadily wresting market share from Chinese brands in their home market. In response, China's mostly state-owned automakers are on a campaign to preserve protectionist policies. PAGE B1

INTERNATIONAL A3-9

New Lead in Jet Search

In what an official called "a great lead," an Australian vessel detected two sets of signals that might originate from recorders of missing Flight 370. PAGE A3

A Smoother Afghan Election

Last weekend's vote did not have the widespread complaints of fraud that marred the election of 2009. PAGE A4

NEW YORK A16-21

Unseen Evidence in 1985 Case

Notes found in a review of work by a Brooklyn detective could exonerate two men convicted of a killing. PAGE A16

NATIONAL A10-15

Accord on Jobs for the Disabled

The Justice Department and Rhode Island reached a deal to give people with developmental disabilities opportunities in the competitive workplace. PAGE A10

Shift on Award to Islam Critic

Brandeis University said it would not give an honorary degree to Ayaan Hirsi Ali, a fierce critic of Islam. PAGE A10

SPORTSWEDNESDAY B12-18

An N.B.A. Farming Concept

The Miami Heat have forged an alliance with a developmental team in, of all places, South Dakota. PAGE B12

DINING D1-8

No Delivery Required

Pizza made at home can be better and less expensive than any pie ordered in. Sam Sifton offers a guide from dough to toppings. PAGE D1

ARTS C1-8

Behind the Updike Charm

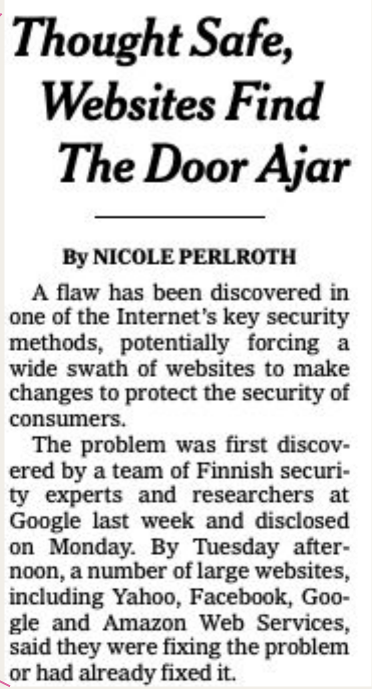
A new biography of the novelist John Updike looks beyond his public image. A review by Dwight Garner. PAGE C1

Aftermath of an Attack

Sergei Filin, artistic director of the Bolshoi Ballet, talked about his recovery from a brutal acid attack. PAGE C1

EDITORIAL, OP-ED A22-23

Thomas L. Friedman PAGE A23



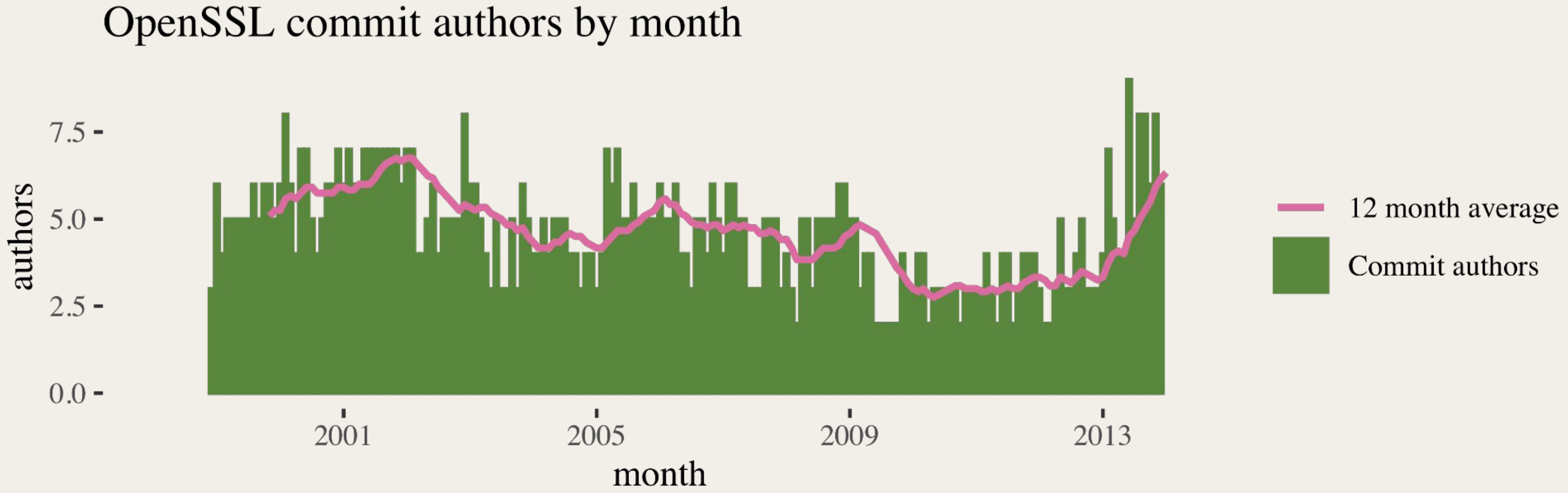
Thought Safe, Websites Find The Door Ajar

By NICOLE PERLROTH

A flaw has been discovered in one of the Internet's key security methods, potentially forcing a wide swath of websites to make changes to protect the security of consumers.

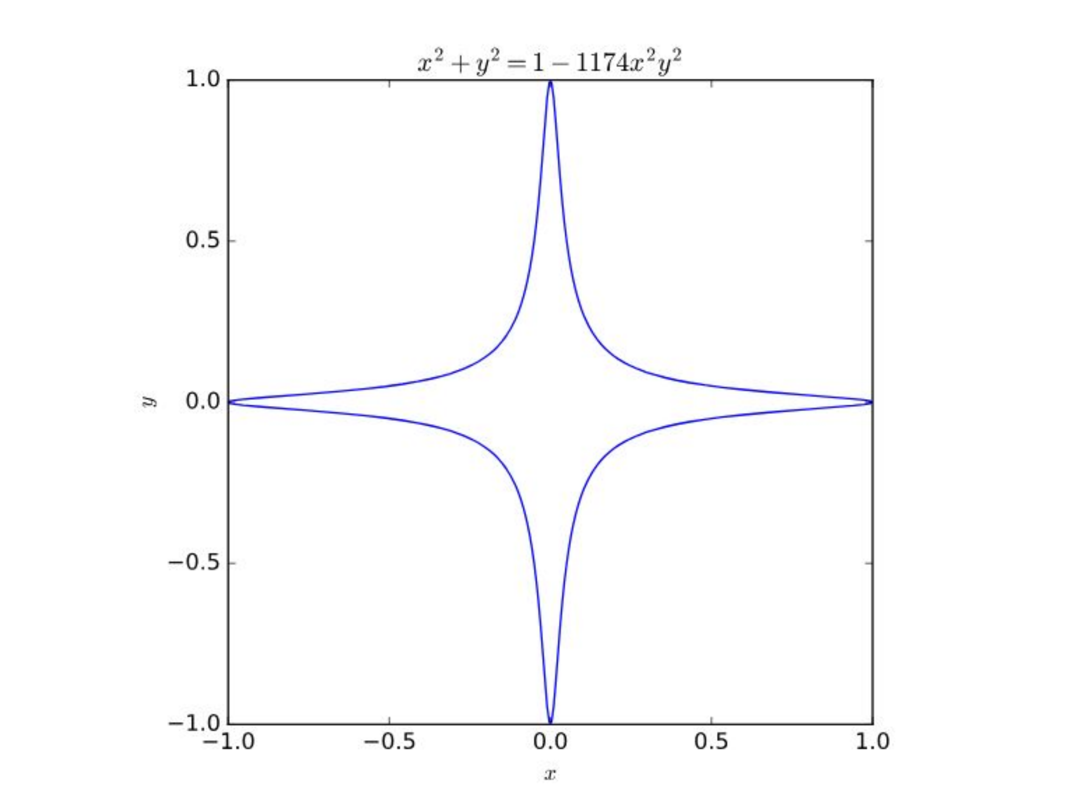
The problem was first discovered by a team of Finnish security experts and researchers at Google last week and disclosed on Monday. By Tuesday afternoon, a number of large websites, including Yahoo, Facebook, Google and Amazon Web Services, said they were fixing the problem or had already fixed it.

The OpenSSL's community wasn't keeping up



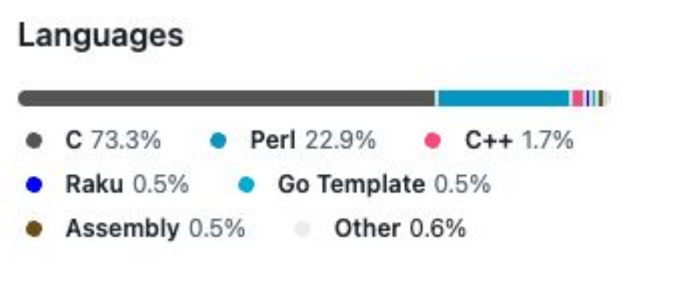
The OpenSSL community (pre-Heartbleed)

Cryptography can be intimidating



https://www.johndcook.com/blog/2019/02/19/addition-on-curve1174/

Not everyone can contribute code



Languages

● C 73.3% ● Perl 22.9% ● C++ 1.7%

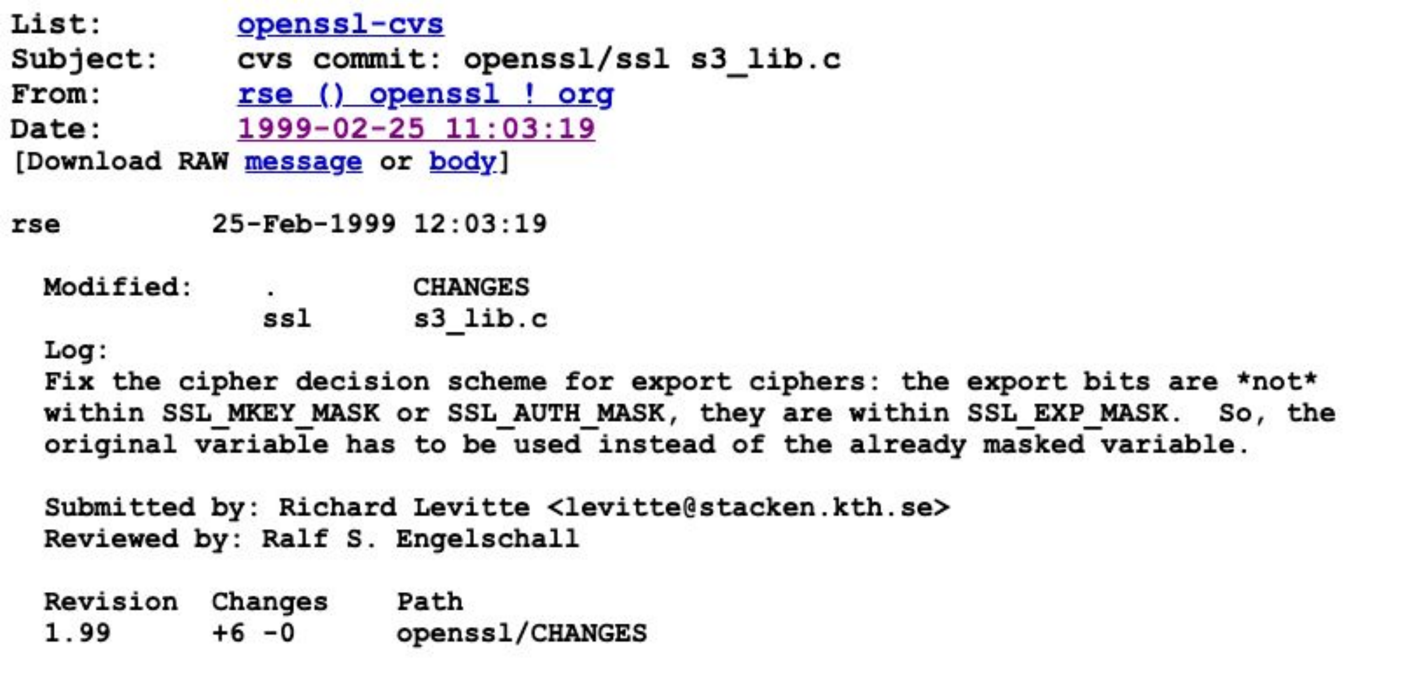
● Raku 0.5% ● Go Template 0.5%

● Assembly 0.5% ● Other 0.6%

Note: a lot of the Perl code exists to generate assembly code:

```
$code .= <<___;

.p2align 3

.globl ossl_md5_block_asm_data_order@{[$isaext]}

.type ossl_md5_block_asm_data_order@{[$isaext]},\@function

ossl_md5_block_asm_data_order@{[$isaext]}:
```

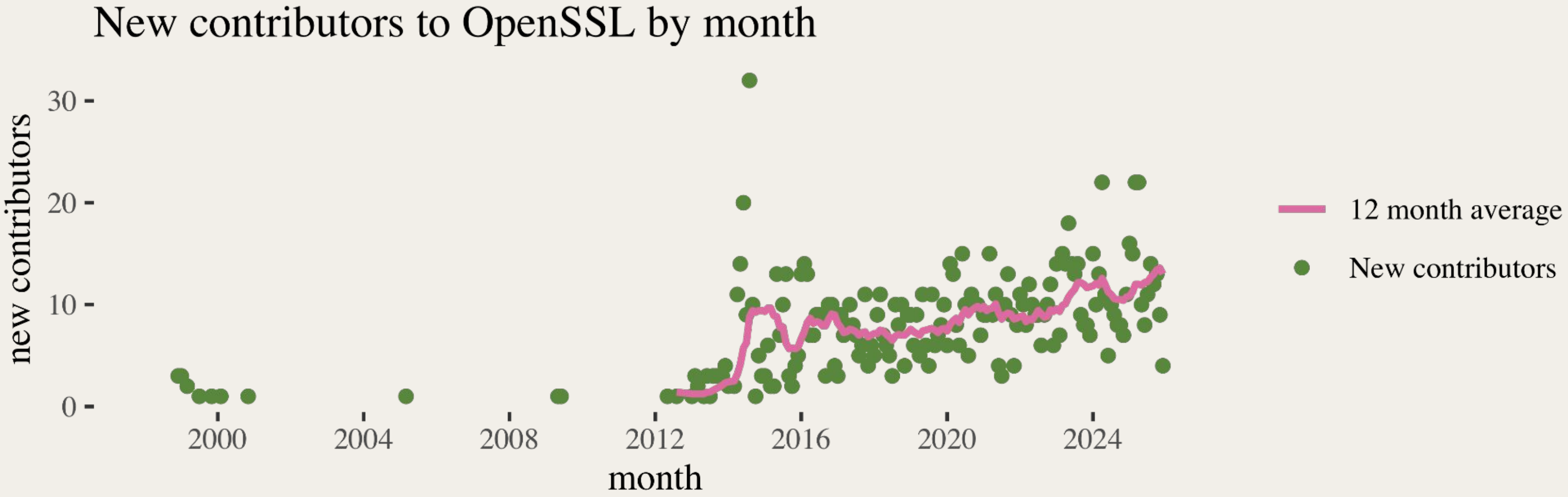
Community via mailing lists



```
List:         openssl-cvs
Subject:      cvs commit: openssl/ssl s3_lib.c
From:         rse () openssl ! org
Date:         1999-02-25 11:03:19
[Download RAW message or body]

rse          25-Feb-1999 12:03:19

  Modified:     .          CHANGES
               ssl         s3_lib.c
  Log:
  Fix the cipher decision scheme for export ciphers: the export bits are *not*
  within SSL_MKEY_MASK or SSL_AUTH_MASK, they are within SSL_EXP_MASK.  So, the
  original variable has to be used instead of the already masked variable.

  Submitted by: Richard Levitte <levitte@stacken.kth.se>
  Reviewed by: Ralf S. Engelschall

  Revision  Changes    Path
  1.99      +6 -0      openssl/CHANGES
```

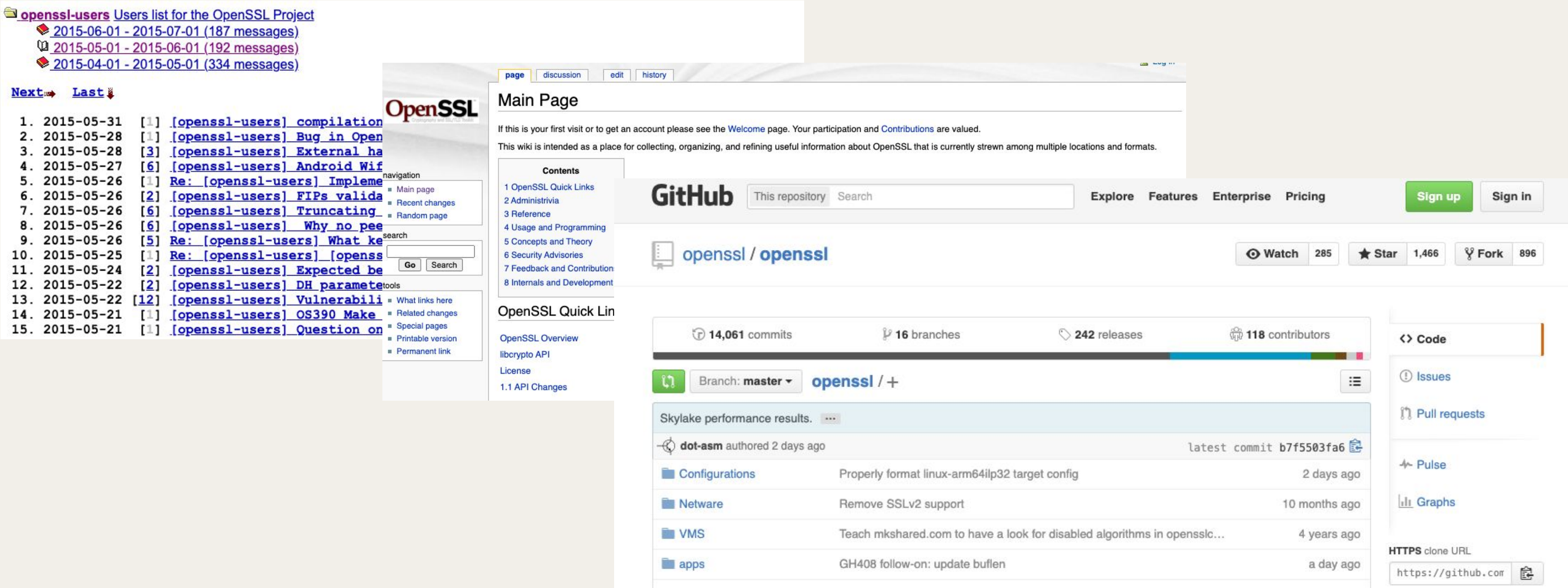
The larger community

Healthy communities bring in new people



People like to see order

OpenSSL community in 2015



openssl-users Users list for the OpenSSL Project

- 2015-06-01 - 2015-07-01 (187 messages)
- 2015-05-01 - 2015-06-01 (192 messages)
- 2015-04-01 - 2015-05-01 (334 messages)

Next Last

```
 1. 2015-05-31   [1] [openssl-users] compilation
 2. 2015-05-28   [1] [openssl-users] Bug in Open
 3. 2015-05-28   [3] [openssl-users] External ha
 4. 2015-05-27   [6] [openssl-users] Android Wif
 5. 2015-05-26   [1] Re: [openssl-users] Impleme
 6. 2015-05-26   [2] [openssl-users] FIPs valida
 7. 2015-05-26   [6] [openssl-users] Truncating
 8. 2015-05-26   [6] [openssl-users]  Why no pee
 9. 2015-05-26   [5] Re: [openssl-users] What ke
10. 2015-05-25   [1] Re: [openssl-users] [openss
11. 2015-05-24   [2] [openssl-users] Expected be
12. 2015-05-22   [2] [openssl-users] DH paramete
13. 2015-05-22  [12] [openssl-users] Vulnerabili
14. 2015-05-21   [1] [openssl-users] OS390 Make
15. 2015-05-21   [1] [openssl-users] Question on
```

Main Page

If this is your first visit or to get an account please see the Welcome page. Your participation and Contributions are valued.

This wiki is intended as a place for collecting, organizing, and refining useful information about OpenSSL that is currently strewn among multiple locations and formats.

Contents

1 OpenSSL Quick Links
2 Administrivia
3 Reference
4 Usage and Programming
5 Concepts and Theory
6 Security Advisories
7 Feedback and Contribution
8 Internals and Development

OpenSSL Quick Lin

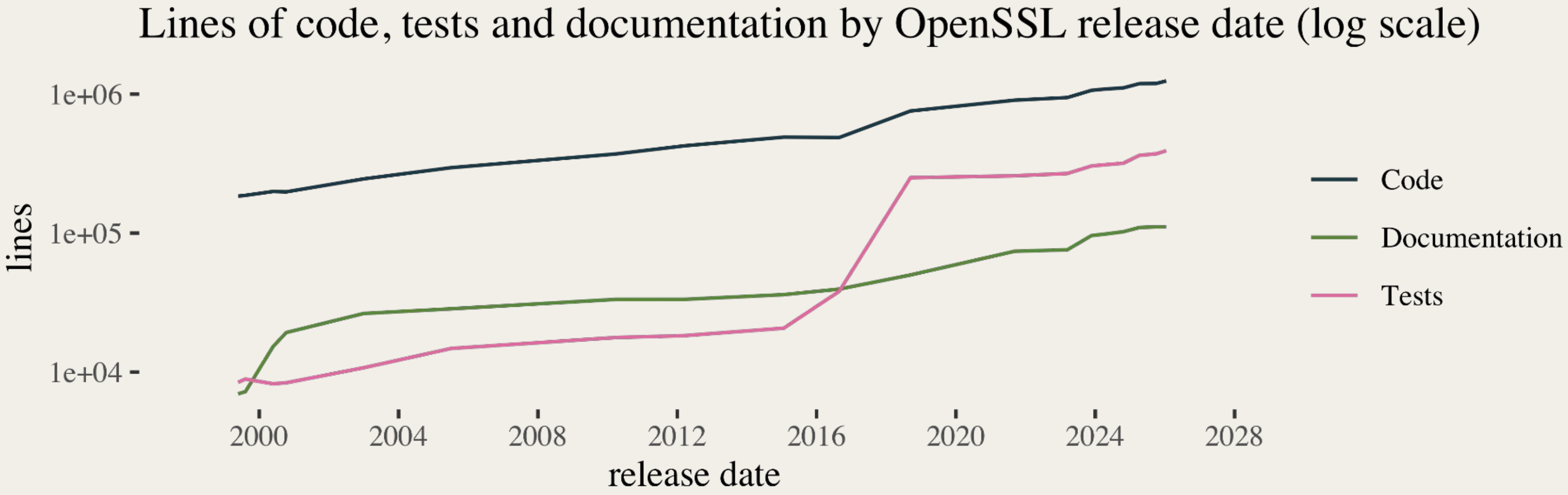
OpenSSL Overview
libcrypto API
License
1.1 API Changes

Skylake performance results. ...

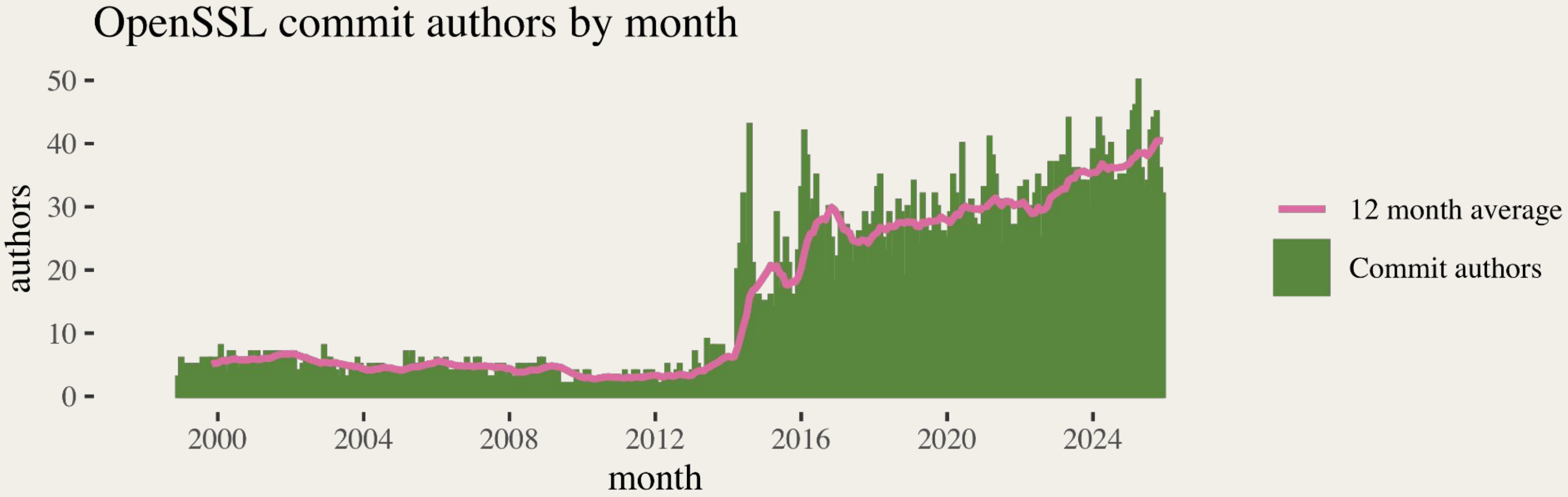
dot-asm authored 2 days ago — latest commit b7f5503fa6

Configurations	Properly format linux-arm64ilp32 target config	2 days ago
Netware	Remove SSLv2 support	10 months ago
VMS	Teach mkshared.com to have a look for disabled algorithms in opensslc…	4 years ago
apps	GH408 follow-on: update buflen	a day ago

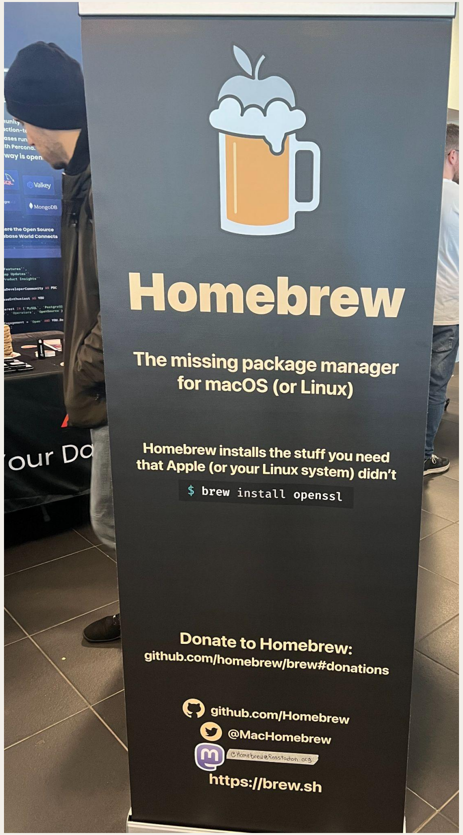
Teasting enables more contributions

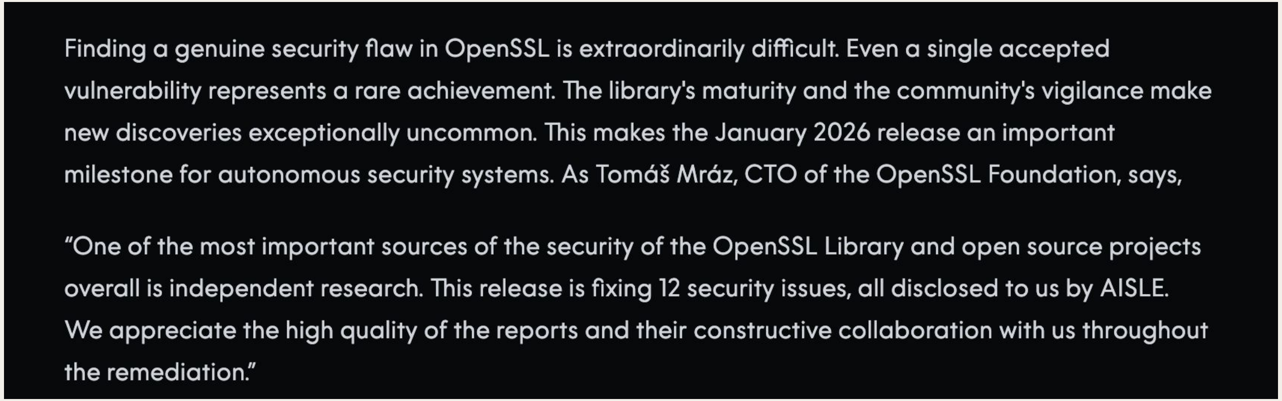


Heartbleed: *good* for the OpenSSL Community



This just in!


Homebrew
The missing package manager for macOS (or Linux)
Homebrew installs the stuff you need that Apple (or your Linux system) didn't
$ brew install openssl
Donate to Homebrew:
github.com/homebrew/brew#donations
github.com/Homebrew
@MacHomebrew
@Homebrew@fosstodon.org
https://brew.sh



Finding a genuine security flaw in OpenSSL is extraordinarily difficult. Even a single accepted vulnerability represents a rare achievement. The library's maturity and the community's vigilance make new discoveries exceptionally uncommon. This makes the January 2026 release an important milestone for autonomous security systems. As Tomáš Mráz, CTO of the OpenSSL Foundation, says,

“One of the most important sources of the security of the OpenSSL Library and open source projects overall is independent research. This release is fixing 12 security issues, all disclosed to us by AISLE. We appreciate the high quality of the reports and their constructive collaboration with us throughout the remediation.”

Thank you to our leading supporters!

PREMIER SUPPORTERS

openSSL CORPORATION

cisco

Sovereign Tech Fund

FLOSS/fund
by ZERODHA

CODE PROTECTORS

NetApp

COMCAST

Two Qs

?

The OpenSSL Foundation Mission

The OpenSSL Foundation works to ensure that **everyone**, including nonprofits, academics, and independent developers, **has access to fundamental data privacy and security tools** that are the backbone of internet protection, quietly safeguarding millions of users. We do this to help build a safer internet — one that serves the public interest and upholds **privacy and security as foundational rights**.

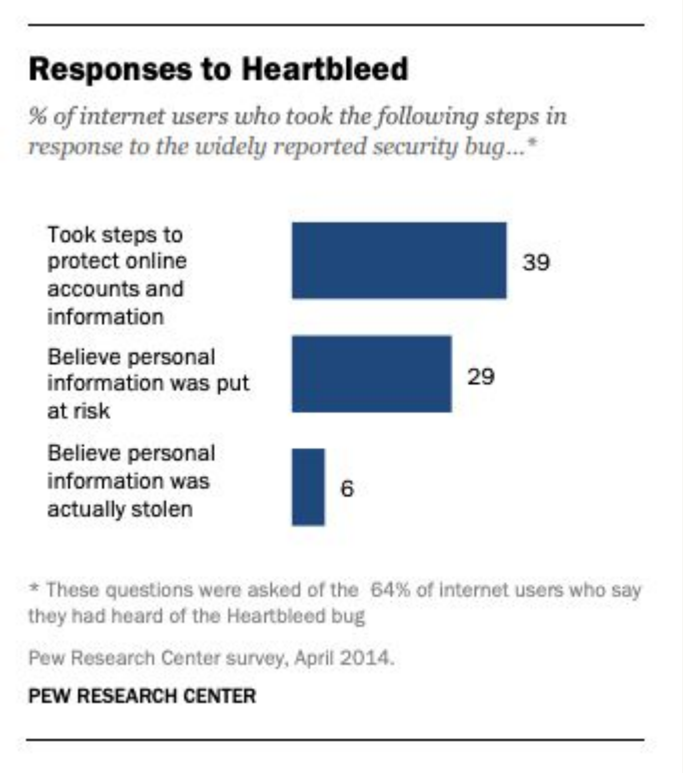
Here be dragons!

https://en.wikipedia.org/wiki/Here_be_dragons

Heartbleed

"Heartbleed - the first buffer overflow bug with a website, a logo, and a marketing department."
– Stack Overflow Podcast recorded Friday April 11, 2014

```
if (1 + 2 + payload + 16 > s->s3->rrec.length)
     return 0;
```



Responses to Heartbleed

*% of internet users who took the following steps in response to the widely reported security bug...**

* These questions were asked of the 64% of internet users who say they had heard of the Heartbleed bug

Pew Research Center survey, April 2014.

PEW RESEARCH CENTER

Turns out there's money in support contracts

What motivates open source contributors?

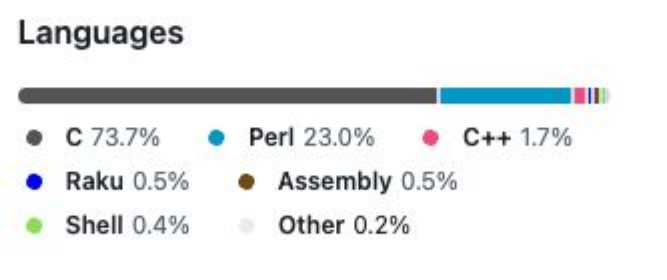
- Scratch your own itch!

Version 3.0
for Windows 95/Windows NT
US and Canada Only - Not For Export

Disk 3 of 4

What motivates open source contributors?

- Scratch your own itch!
- Interesting problems



Languages

● C 73.7% ● Perl 23.0% ● C++ 1.7%

● Raku 0.5% ● Assembly 0.5%

● Shell 0.4% ● Other 0.2%

What motivates open source contributors?

- Scratch your own itch!
- Interesting problems
- It’s your job

What motivates open source contributors?

- Scratch your own itch!
- Interesting problems
- It’s your job
- Someone in the community is helping you get involved!

Open source community undefeated against government and corporate interests

?

This isn’t a zero-sum game

!

1995: Netscape SSL

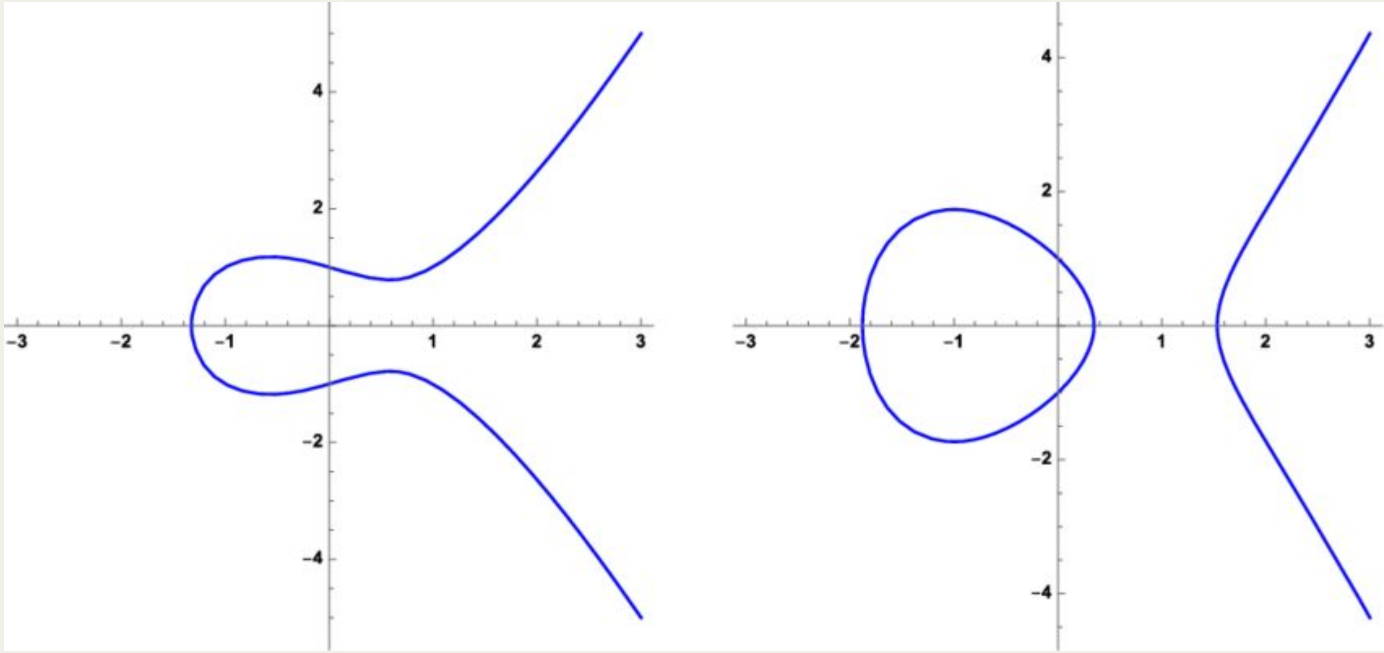
Secured:

- Websites (HTTPS)

Provided

- Encryption algorithms (RSA, RC2, RC4, DES, 3DES and MD5)
- SSL protocol

Cryptography can be intimidating



Elliptic curves. Left: $y^2 = x^3 - x + 1$. Right: $y^2 = x^3 - 3x + 1$

The OpenSSL Library

Secures:

- Websites (HTTPS)
- Email (SNTP with TLS)
- File transfers (FTPS, NNTP, XMPP, SIPS, etc.)
- Voice over Internet Protocol (VoIP)
- Virtual Private Network (OpenVPN, OpenConnect)
- Other stuff . . .

Provides:

- Arbitrary precision integer implementation (BIGNUM)
- A full-feature cryptography library
- TLS/SSL and QUIC protocol library
- Platform for third-parties providers