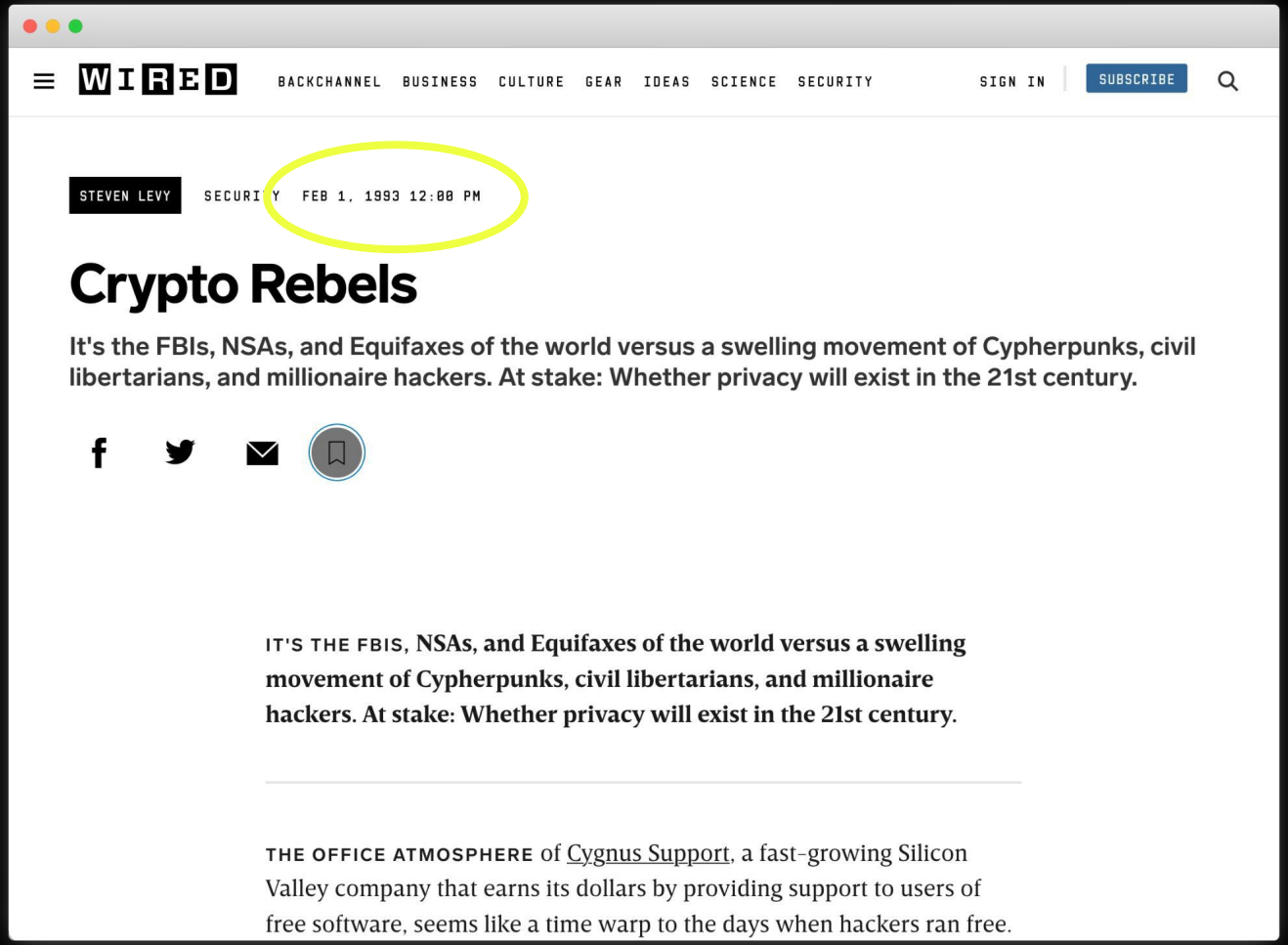
Victims Of Our Success

How open source vulnerabilities became a national security risk

Aeva Black
T: @AevaVoom | W: https://aeva.online

Secretary of the Board, Open Source Initiative
Vice Chair, OpenSSF Technical Advisory Committee



https://www.wired.com/1993/02/crypto-rebels/

Statement by Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger on President Biden's Cyber Executive Order

MARCH 08, 2022 • STATEMENTS AND RELEASES

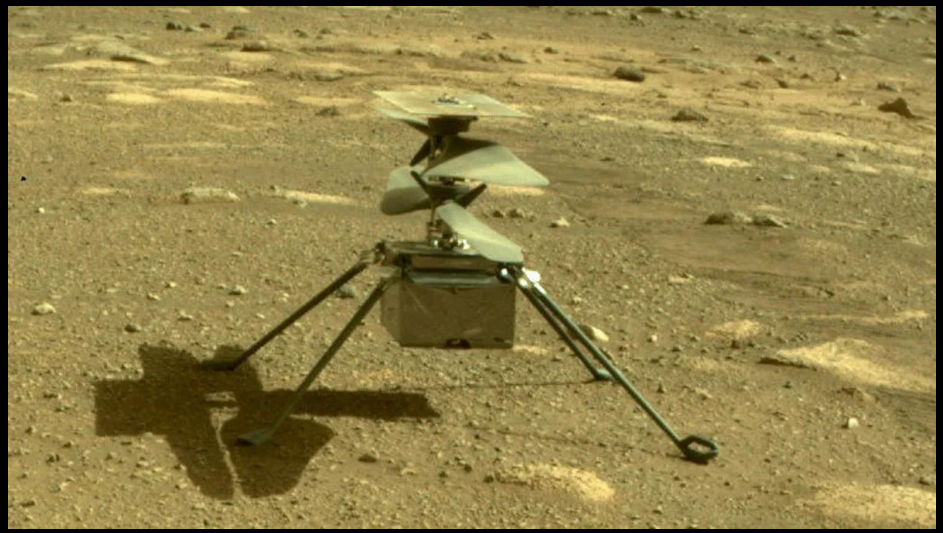
The President's Executive Order, *Improving the Nation's Cybersecurity*, charted a new course for nation's cybersecurity. And, we have begun implementation of one of the most important components of the Executive Order. As of yesterday, every company that sells software to the government must have a rigorous software security program in place. The requirement covers traditional commercial on-premise software, software provided as a service, as well as any included open source software components.

Top

“Am I safe?”

OSS is
everywhere

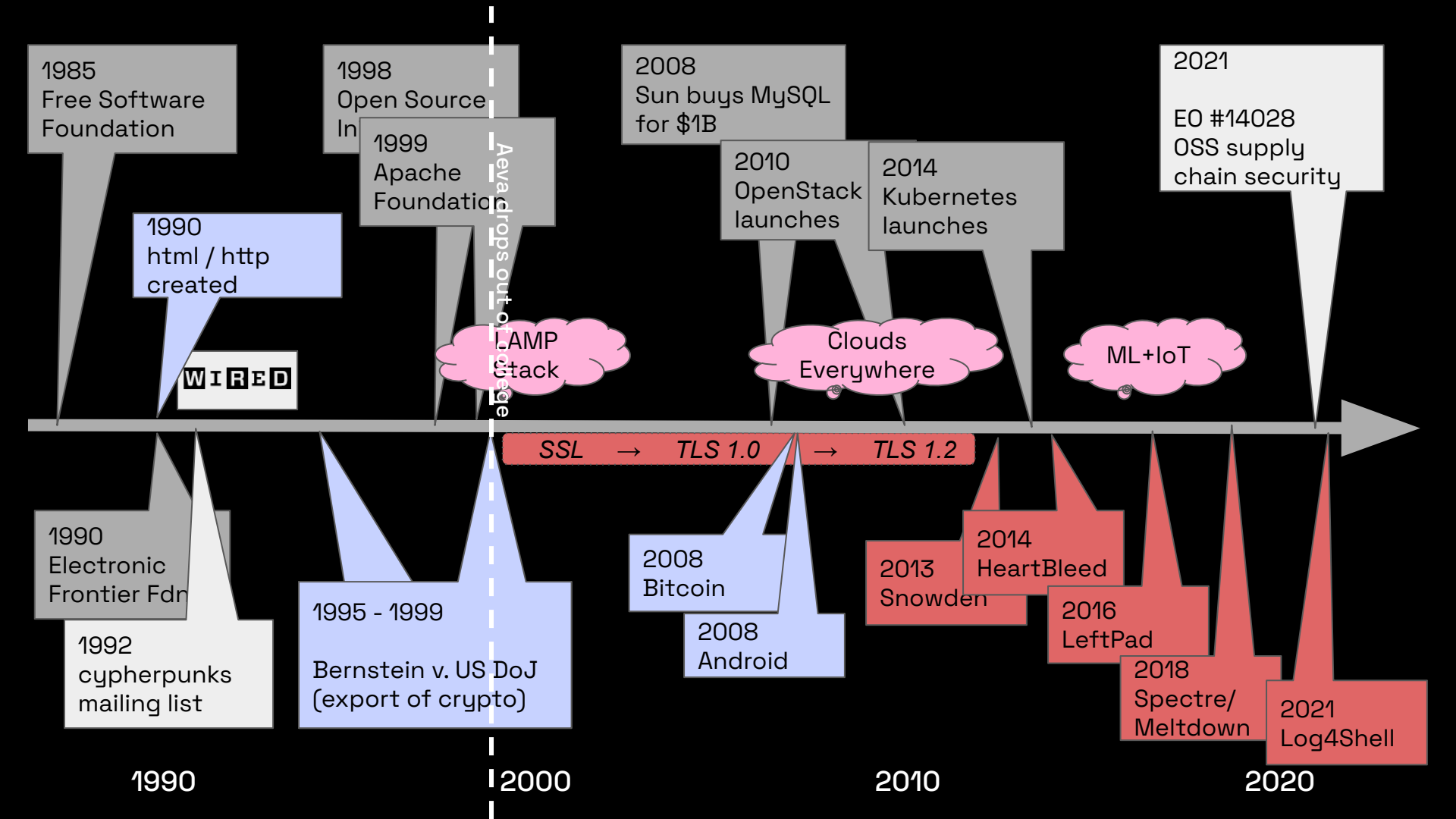
Even On Mars!



https://www.zdnet.com/article/flying-on-mars-fueled-with-open-source-software/

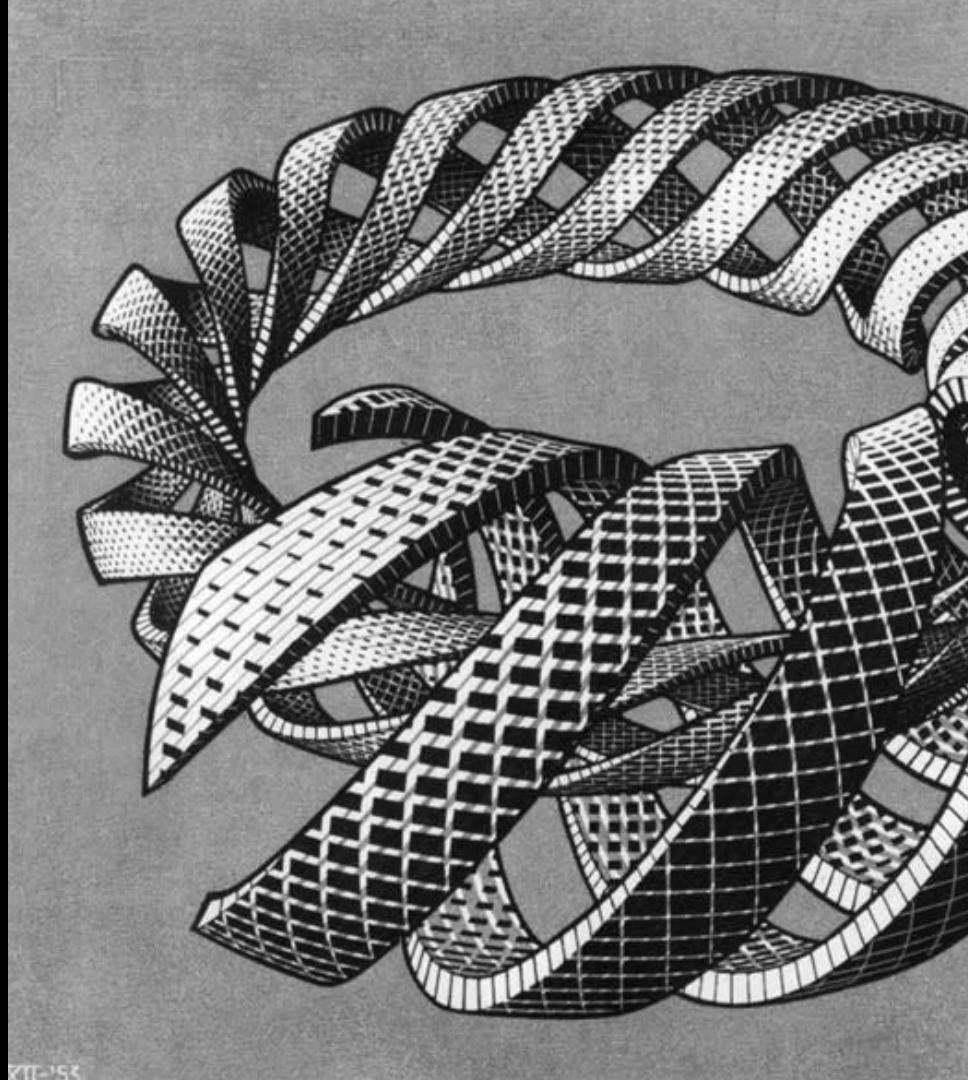
OSS is
everywhere

... however ...


1985
Free Software
Foundation
1998
Open Source
In
1999
Apache
Foundation
Aeva drops out of college
2008
Sun buys MySQL
for $1B
2010
OpenStack
launches
2014
Kubernetes
launches
2021
EO #14028
OSS supply
chain security
1990
html / http
created
WIRED
LAMP
Stack
Clouds
Everywhere
ML+IoT
SSL → TLS 1.0 → TLS 1.2
1990
Electronic
Frontier Fdn
1992
cypherpunks
mailing list
1995 - 1999
Bernstein v. US DoJ
(export of crypto)
2008
Bitcoin
2008
Android
2013
Snowden
2014
HeartBleed
2016
LeftPad
2018
Spectre/
Meltdown
2021
Log4Shell
1990
2000
2010
2020

What’s changed?

The solution to today's problem is destined to become tomorrow's problem.



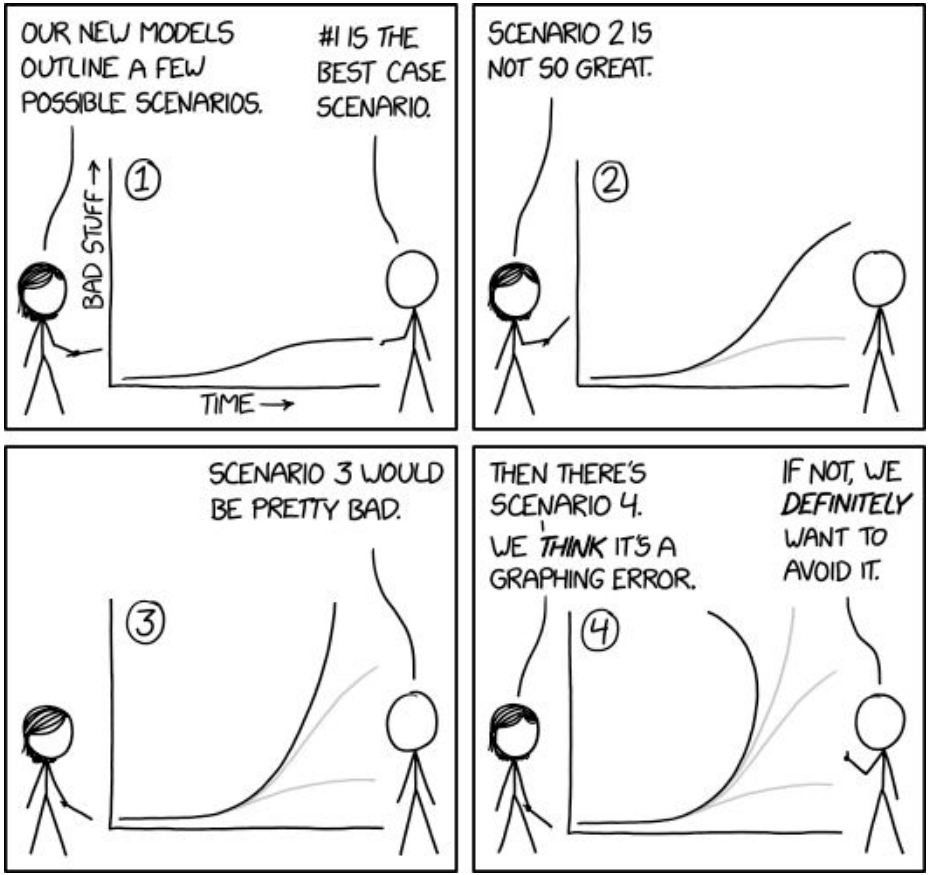
“Any sufficiently advanced technology is indistinguishable from magic.”

– Arthur C. Clarke

Magicians & Apprentices

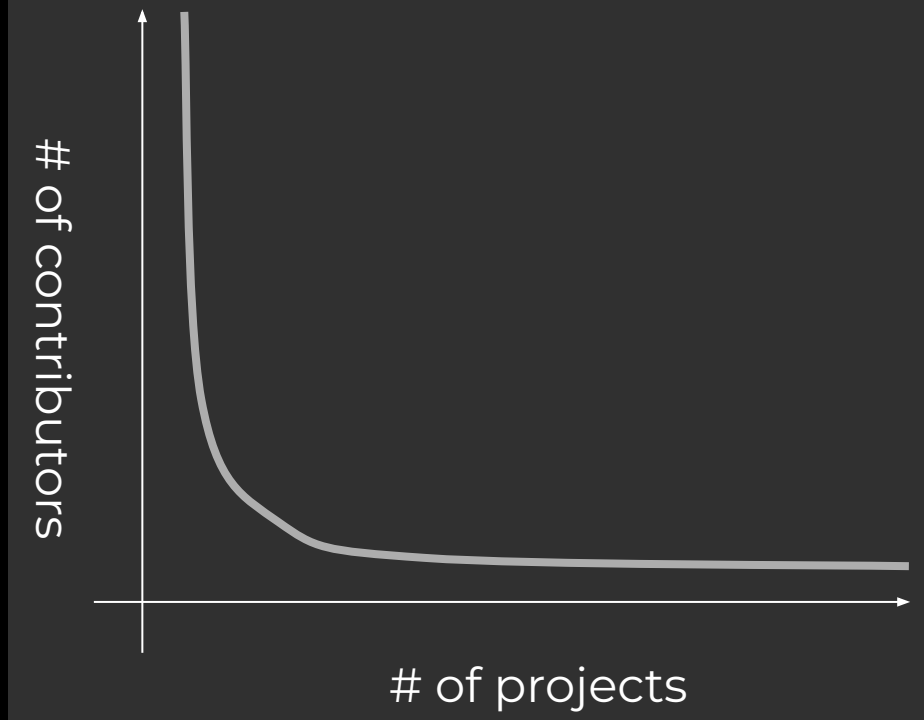
Contribution to, and usage of, Open Source Software has grown exponentially...

and outpaced our transmission of institutional knowledge.

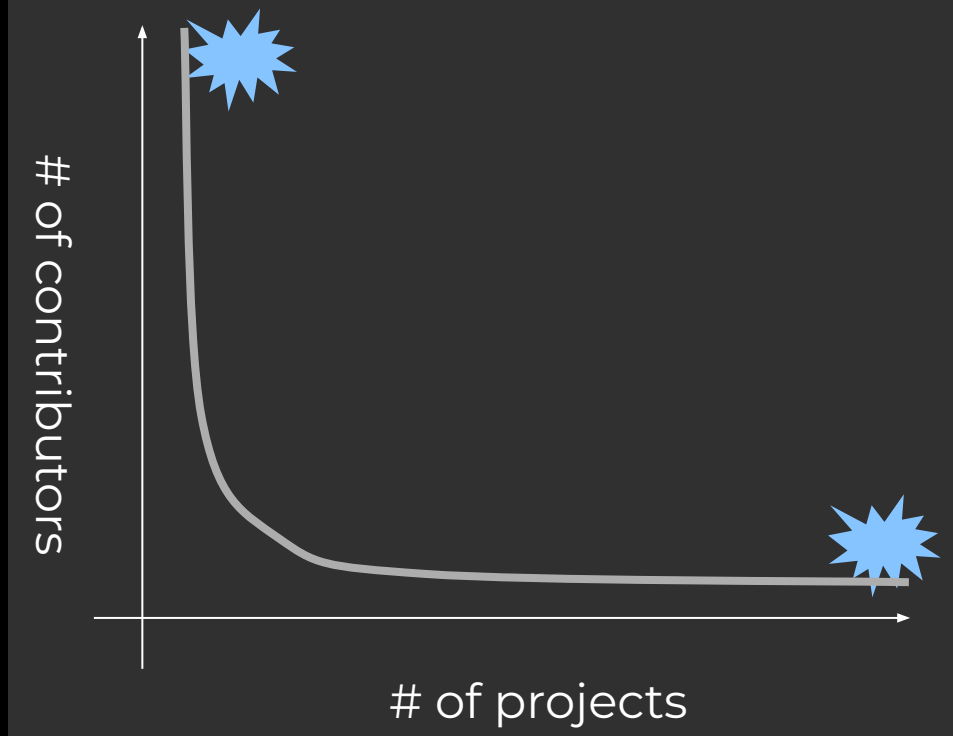


Mean contributor per project:

~1

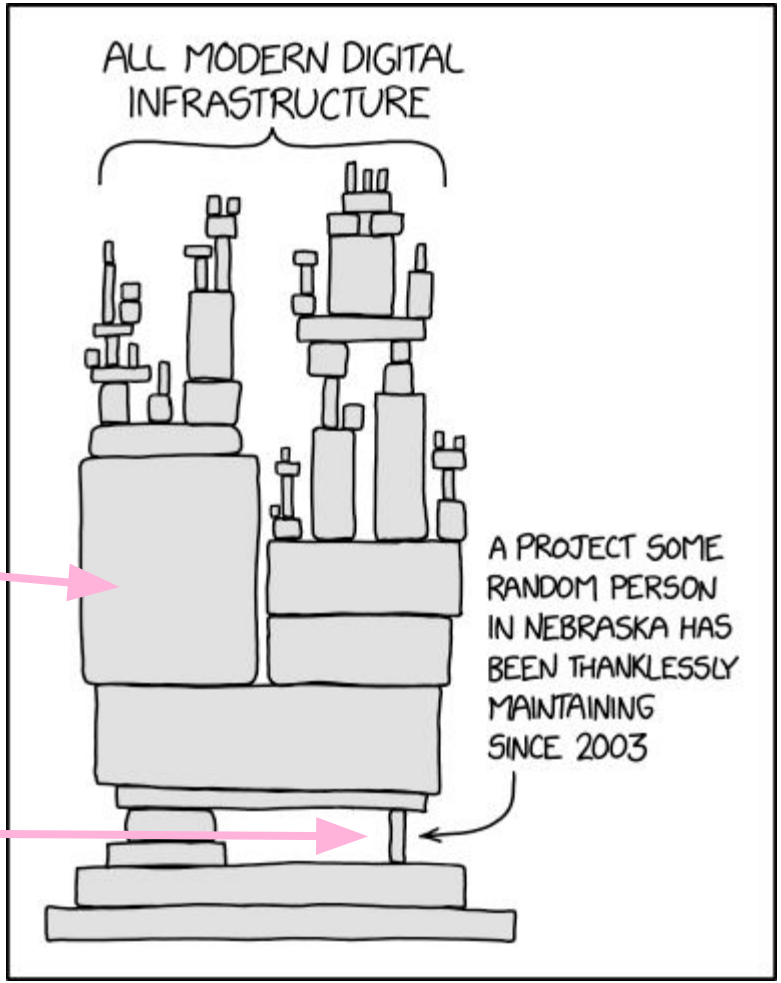


Different Problems At Different Scales



kubernetes

log4j



What's **hasn't** changed?

Human Scalability

Robin Dunbar

(anthropologist dude)

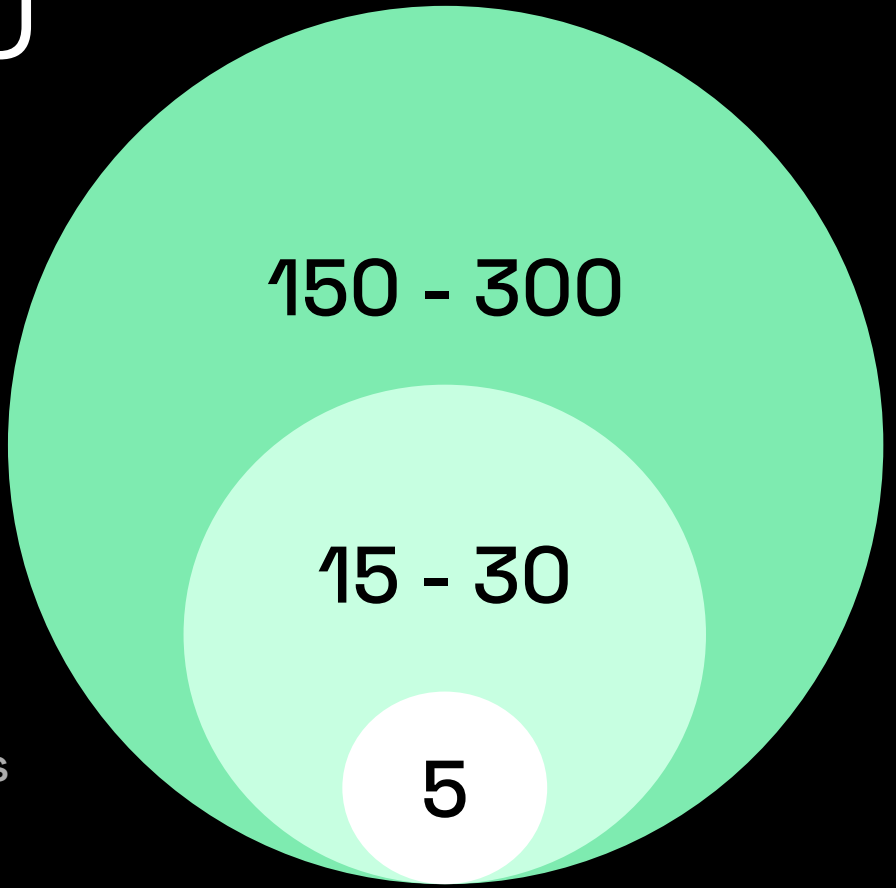
https://en.wikipedia.org/wiki/Robin_Dunbar

Dunbar's Number(s)

You remember their name.
Might remember their project or other random facts.

Confident in shared goals

Often finish each other's sentences



Constraints On Group Size

(even in the digital age)

"[T]here is a cognitive constraint on the size of social networks that even the communication advantages of online media are unable to overcome.

In practical terms, it may reflect the fact that real (as opposed to casual) relationships require at least occasional face-to-face interaction to maintain them."

https://royalsocietypublishing.org/doi/10.1098/rsos.150292

Trust

Trust

Trust

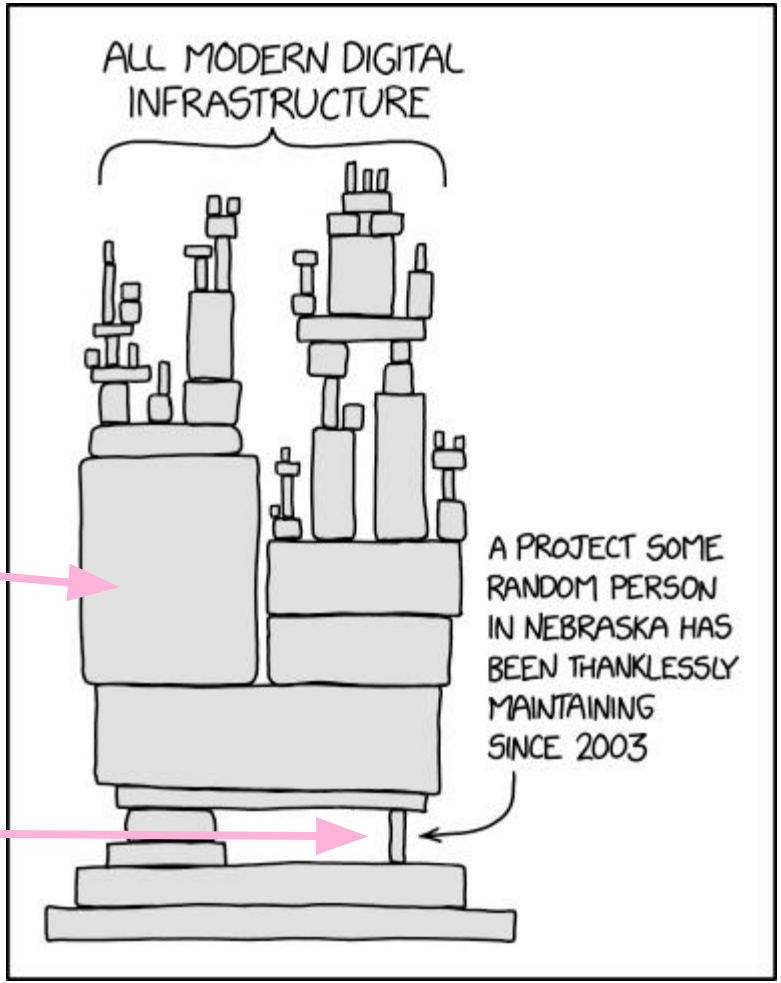
“[trust] is not a property, but rather
an assessment based on experience...

[It is] a declaration made by an observer
[not] a property of the observed.”

– Dorothy Denning, 1993

kubernetes

log4j



Four Opens

Four Freedoms

Four Opens

- Open Source
- Open Design
- Open Development
- Open Community

Four Freedoms

- To run it
- To redistribute it
- To study and change it
- To share your changes

Four Opens

describe how we can
build it together

Four Freedoms

describe what we can
do with it individually

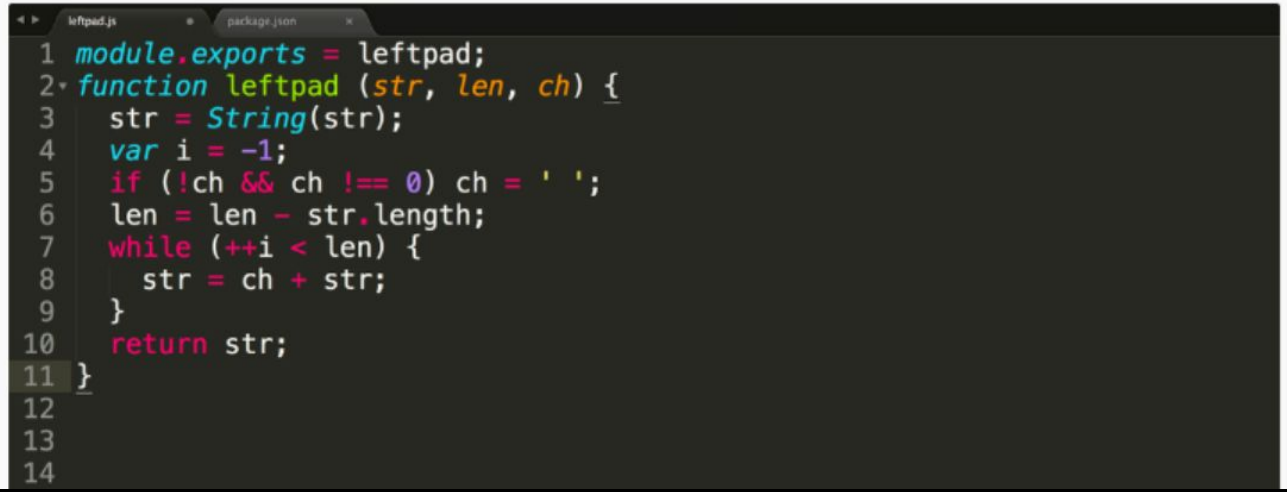
How About Some Examples

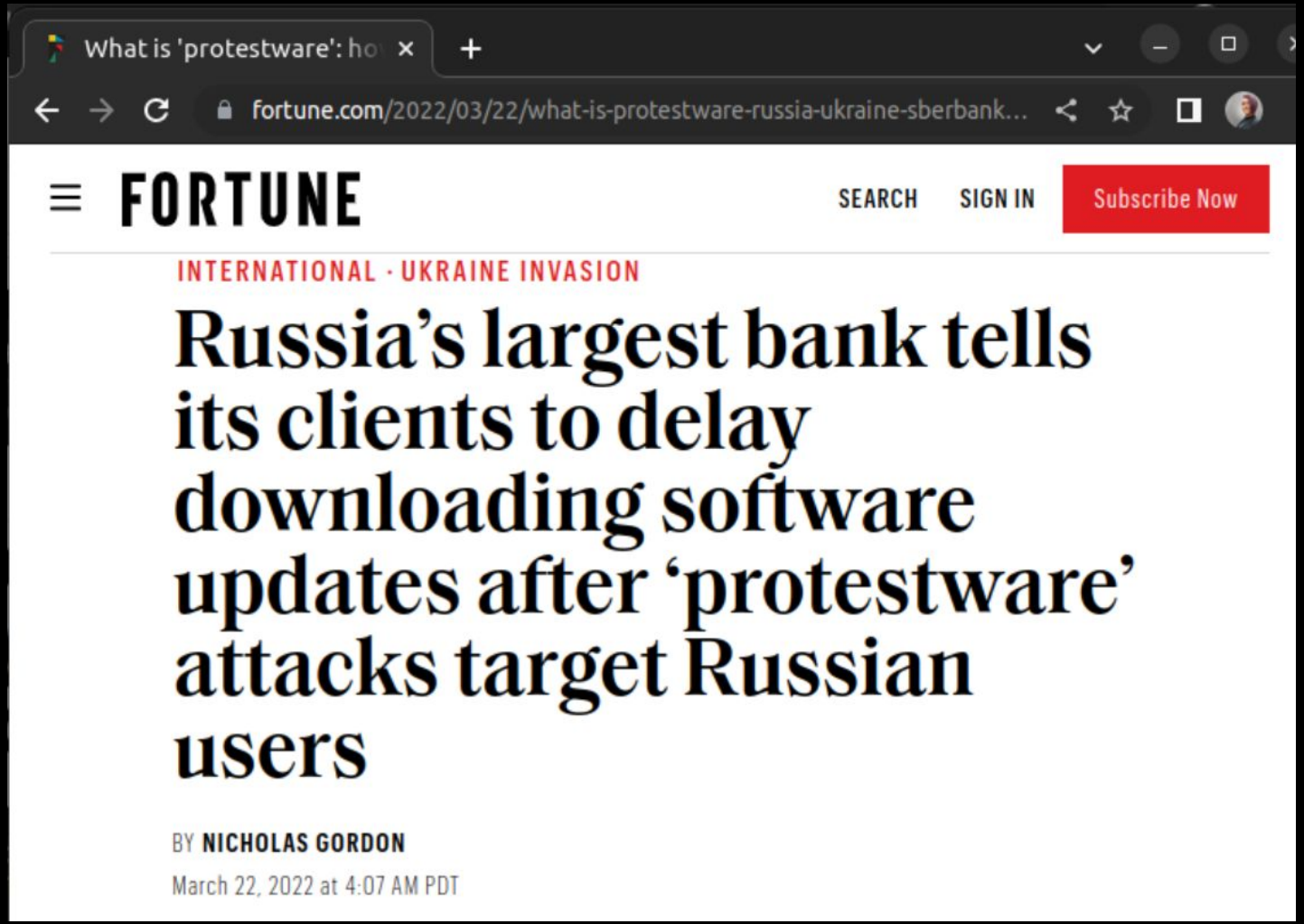
QZ How one programmer br ×

qz.com/646467/how-one-programmer-broke-the-internet-by-deleting-a-tin...

QUARTZ

How one programmer broke the internet by deleting a tiny piece of code




What is 'protestware': ho
fortune.com/2022/03/22/what-is-protestware-russia-ukraine-sberbank...
FORTUNE
SEARCH
SIGN IN
Subscribe Now
INTERNATIONAL · UKRAINE INVASION
Russia's largest bank tells its clients to delay downloading software updates after 'protestware' attacks target Russian users
BY NICHOLAS GORDON
March 22, 2022 at 4:07 AM PDT

What You Can Do

We Need To Adapt

with new tools for open source software creation & consumption

- 51% of organizations don't have a security policy for open source development or usage.

- 30% of [those] organizations … recognize that no one on their team is responsible for addressing open source security.

https://openssf.org/blog/2022/06/21/state-of-open-source-security-2022-from-snyk-and-the-linux-foundation

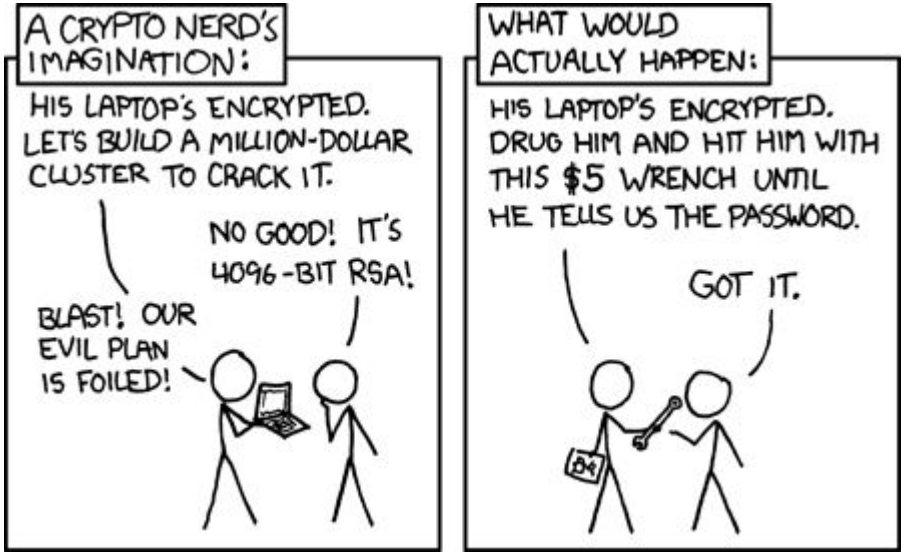
Individual's Responsibility

If your project becomes popular / is used in something popular...

- Act responsibly; your actions affect others & reflect on us all.
- Don't be the weak link; protect yourself with 2FA, good PKI hygiene, signed commits, etc.
- Don't work alone; seek collaborators.

No, Really.

You are a potential vector for hostile (state) actors.



“What about those projects with just a few maintainers?”

Industry's Responsibility

Whether funding contributors or integrating OSS into products...

- Recognize your choice to externalize your risk budget.
- Include OSS in your budget: if you can't "afford" it, don't consume it.
- The Cost Of Goods is hidden in your staff, maintenance, and security budgets. You'll get a better ROI by spending some upstream.

Industry's Responsibility

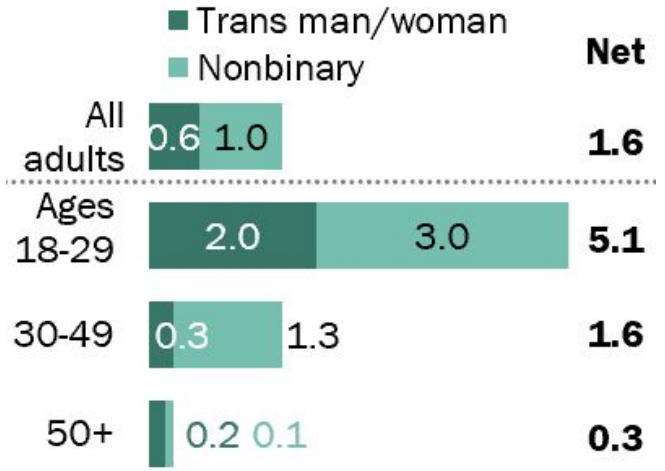
(part two)

- Align incentives to create stable OSS infrastructure; no one wants a bridge that falls over in 5-10 years.
- Consider ethical implications when building/releasing OSS. (Or really any product.)

Closing Thoughts

Demographics are changing

Foster diversity in your communities in order to sustain OSS through the next generation of contributors



Note: Trans men are those who said they were assigned female at birth and described their gender as a man. Trans women are those who said they were assigned male at birth and described their gender as a woman. Figures may not add to subtotals due to rounding.
Source: Survey of U.S. adults conducted May 16-22, 2022.

PEW RESEARCH CENTER

https://www.pewresearch.org/fact-tank/2022/06/07/about-5-of-young-adults-in-the-u-s-say-their-gender-is-different-from-their-sex-assigned-at-birth

4.

IMPRESSIO LIBRORVM.

Potest vt vna vox capi aure plurima: Limunt ita vna scripta mille paginas.

~ FIN ~