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
Crypto Rebels

It's the FBIs, NSAs, and Equifaxes of the world versus a swelling movement of Cypherpunks, civil libertarians, and millionaire hackers. At stake: Whether privacy will exist in the 21st century.

THE OFFICE ATMOSPHERE of Cygnus Support, a fast-growing Silicon Valley company that earns its dollars by providing support to users of free software, seems like a time warp to the days when hackers ran free.
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.
“Am I safe?”
OSS is everywhere

Even On Mars!

OSS is everywhere

... however ...
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
ALL MODERN DIGITAL INFRASTRUCTURE

A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

kubernetes

log4j
What’s hasn’t changed?

Human Scalability
Robin Dunbar

(anthropologist dude)

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
“[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] 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
All modern digital infrastructure

A project some random person in Nebraska has been thanklessly maintaining since 2003

Log4j

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

```javascript
module.exports = leftright;

function leftright(str, len, ch) {
  str = String(str);
  var i = -1;
  if (!ch || ch !== 0) ch = ' ';
  len = len - str.length;
  while (++i < len) {
    str = ch + str;
  }
  return str;
}
```
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.

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

<table>
<thead>
<tr>
<th>Age Range</th>
<th>Trans man/woman</th>
<th>Nonbinary</th>
<th>Net</th>
</tr>
</thead>
<tbody>
<tr>
<td>All adults</td>
<td>0.6</td>
<td>1.0</td>
<td>1.6</td>
</tr>
<tr>
<td>18-29</td>
<td>2.0</td>
<td>3.0</td>
<td>5.1</td>
</tr>
<tr>
<td>30-49</td>
<td>0.3</td>
<td>1.3</td>
<td>1.6</td>
</tr>
<tr>
<td>50+</td>
<td>0.2</td>
<td>0.1</td>
<td>0.3</td>
</tr>
</tbody>
</table>

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.


PEW RESEARCH CENTER

IMPRESSIO LIBRORVM.

Potest ut vna vox capi aure plurima: Linteit ita vna scripta mille paginas.
~ FIN ~