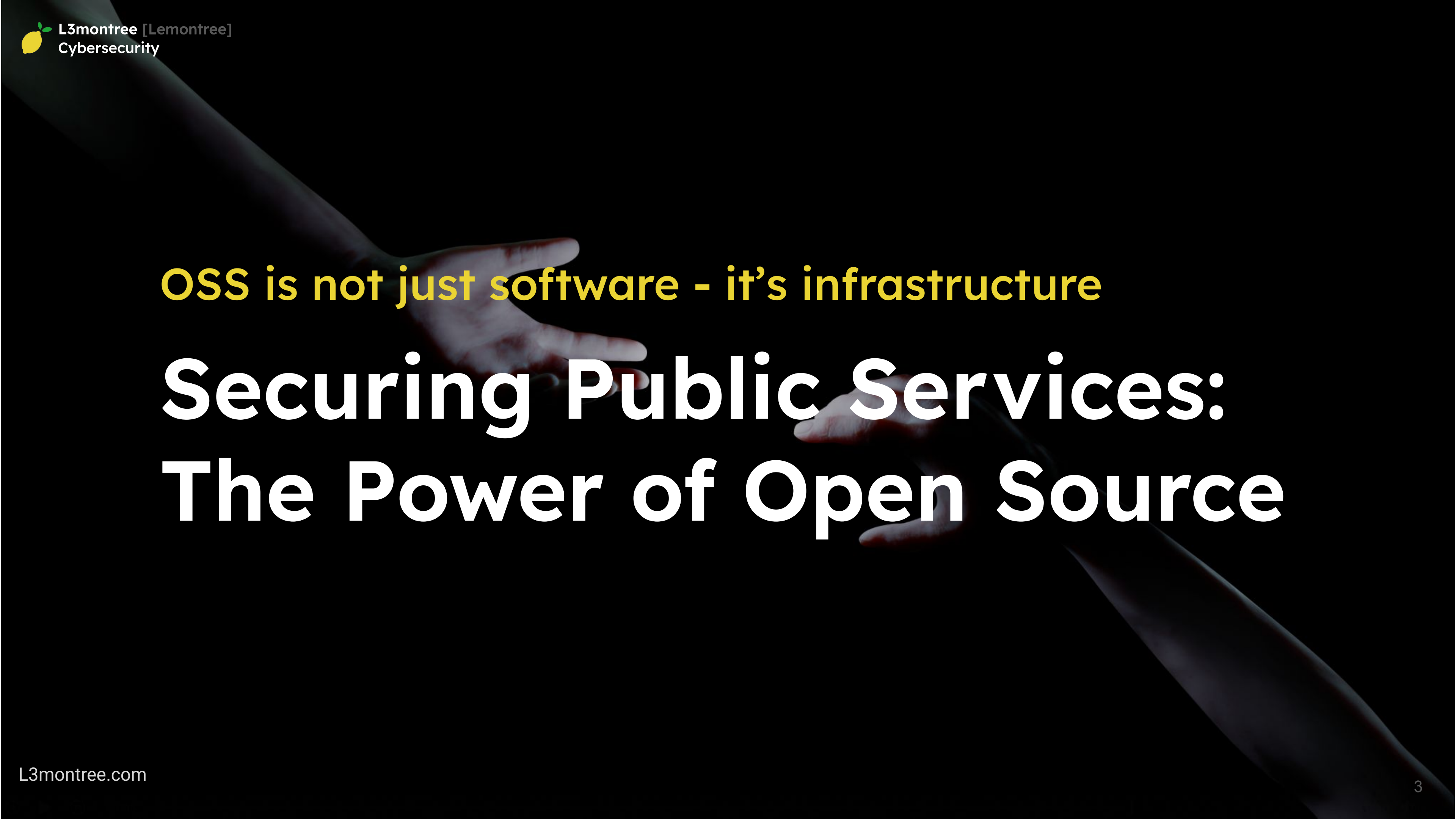
“Open Source Software is inherently insecure.”

“Open Source cannot keep up with typical software.”

“The problem is the so-called Open Source Software.”

Is this belief justified?

Obvious nonsense



OSS is not just software - it’s infrastructure

Securing Public Services: The Power of Open Source

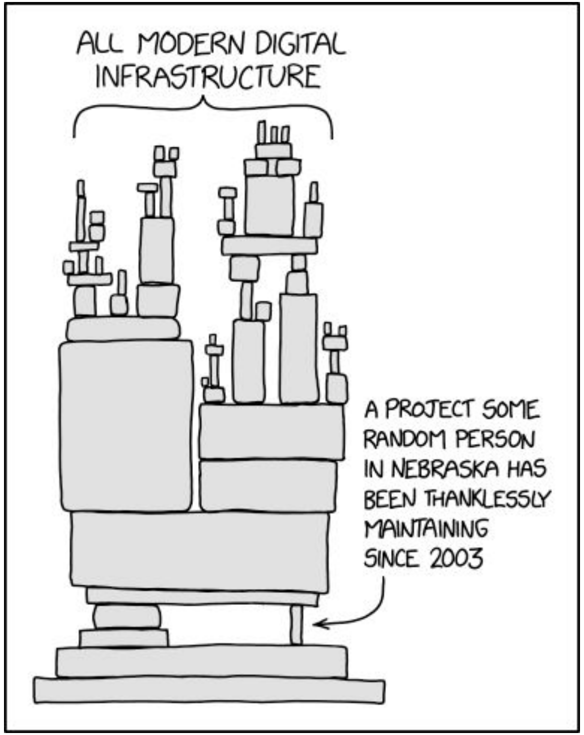
The Reality: Spread and Relevance of OSS

The Reality: Spread and Relevance of OSS

80%-90% of modern software consists of open source software.[1]

[1] The Linux Foundation, Report on the 2020 FOSS Contributor Survey (08.11.24)

The Reality: Spread and Relevance of OSS


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

xkcd “Dependency” (2347)

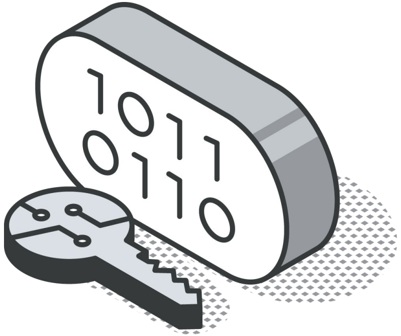
Myth Busting: OSS vs. Proprietary Security

Myth Busting: OSS vs. Proprietary Security

Kerckhoff’s Principle: A secure encryption method must not require secrecy and should be able to fall into enemy hands without damage.

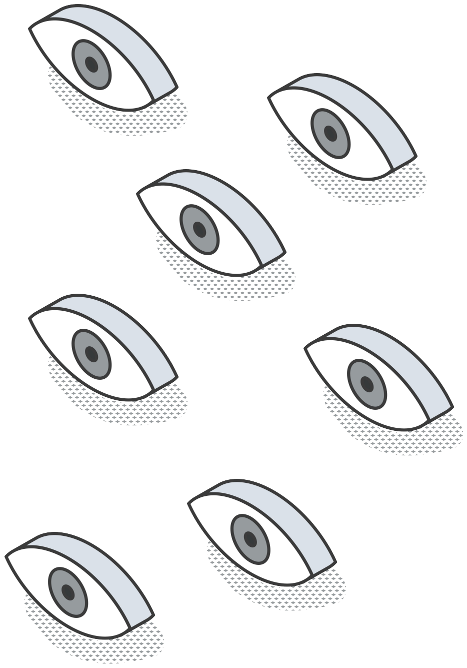
Open Source: e.g. AES/ OpenSSL

Proprietary: Security by obscurity



Based on: Jeff Crume, “Is Open Source More Secure?”, IBM Technology

Myth Busting: OSS vs. Proprietary Security



The more people know a system's details, the more review can be done and the more robust can a system become.

Open Source: Pot. review by many parties

Proprietary: Review solely by the manufacturer

Based on: Jeff Crume, “Is Open Source More Secure?”, IBM Technology

Myth Busting: OSS vs. Proprietary Security

Zen DiS Zentrum Digitale Souveränität

OSS: Quickly identify and eliminate security gaps

P: Relying on processes and speed of manufacturer

OSS: Regularly **check security** requirements

P: Relying on manufacturers statements

OSS: **Eliminate** security gaps **on your own**

P: No development possible, only by manufacturer

Based on: Jutta Horstmann, Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS), "Stellungnahme Anhörung „Open Source" im Ausschuss für Digitales"

Myth Busting: OSS vs. Proprietary Security

Bundesamt
für Sicherheit in der
Informationstechnik

The use of **FLOSS** is associated with **technical and strategic advantages** brought to bear by the freedoms it provides.

FLOSS provides a **basis for IT security**.

- Control to adapt
- Test for vulnerabilities
- Manufacturer independence & Software diversity
- Interoperability

Strategische Position des BSI, www.bsi.bund.de/dok/6604212

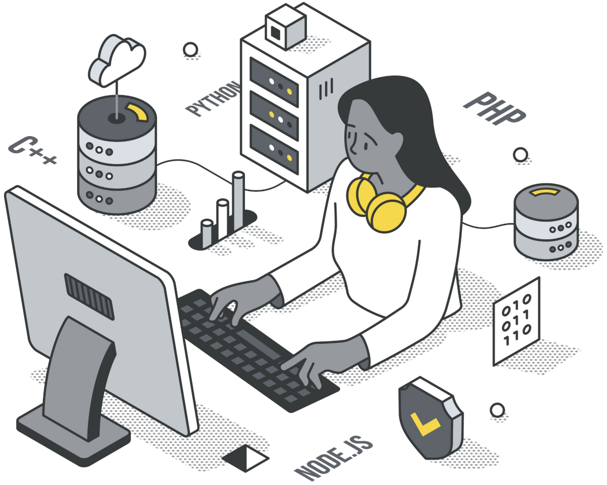
Unique Challenges of OSS Security

Unique Challenges of OSS Security

3 or less

Maintainers for 70% of OSS projects[2]

A lack of active contributing users and a lack of reciprocity among users leaves projects in a difficult state.[3]

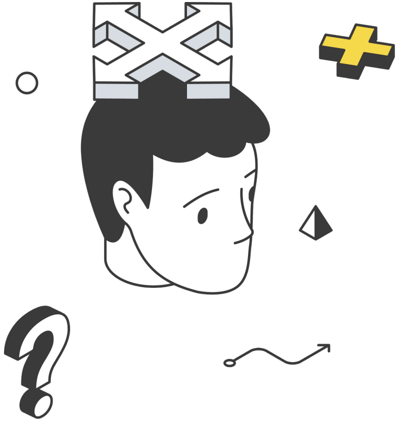


[2]: sovereign.tech/news/what-open-source-maintainers-shared-with-us; [3]: Ryan Ellis, Jaikrishna Bollampalli, “Bug Bounties and FOSS: Opportunities, Risks, and a Path Forward”

Unique Challenges of OSS Security

Contributors avoid security work:
"Because it sucks! It's not fun."

Aaron P. (Core Contributor for Security at Ruby on Rails)



The general challenges of maintaining an open source project are [amplified] by the additional unique challenges associated with security work. [3]

e.g. isolation and reduced collaboration; high-pressure work

[3] Ryan Ellis, Jaikrishna Bollampalli, “Bug Bounties and FOSS: Opportunities, Risks, and a Path Forward”

A Vision for the Future

A Vision for the Future

It is difficult to talk about [...] security [of any Software] without addressing open-source security. Indeed, the two are now inseparable.[3]

#1 **It affects us all – we need to adjust our focus and priorities accordingly.**

[3] 3: Ryan Ellis, Jaikrishna Bollampalli, “Bug Bounties and FOSS: Opportunities, Risks, and a Path Forward”

A Vision for the Future

Contributions are concentrated on a single or small circle of overburdened maintainers.[3]

#2

Improving baseline maintenance capacity leads to security gains.[3]

[3] Ryan Ellis, Jaikrishna Bollampalli, "Bug Bounties and FOSS: Opportunities, Risks, and a Path Forward"

A Vision for the Future

Contributors avoid security work:
"Because it sucks! It's not fun."

Aaron P. (Core Contributor for Security at Ruby on Rails)

#3

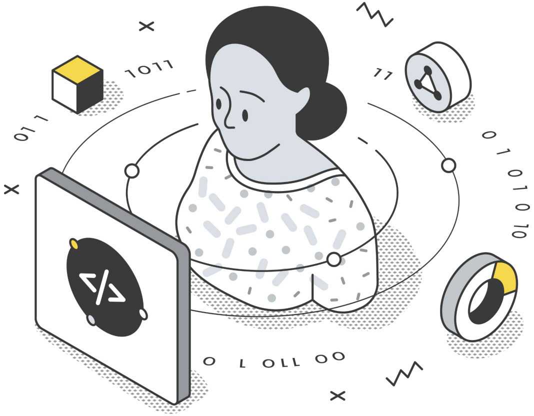
Keep security an active priority: A small number of [good] contractors in a project [can] help manage security; while allowing volunteers to focus on issues they find engaging.[3]

[3] Ryan Ellis, Jaikrishna Bollampalli, "Bug Bounties and FOSS: Opportunities, Risks, and a Path Forward"

A Vision for the Future

The German federal administration paid 197,7 mio. Euro of licence fees to Microsoft in 2023.[4]

This is a vendor lock-in, whereby the state has become vulnerable to blackmailing.



#4

Organizations, companies and public administrations in Europe must fulfil their responsibilities to society and citizens, not least for their own benefit.

[4] heise.de/-9744319

OSS is not just software - it’s infrastructure

If we want secure digital (public) services, strengthening the Open Source Ecosystem is non-negotiable.