

Understanding Trust and Security Processes in the Open Source Software Ecosystem

Dominik Wermke
dwermke.com/enigma

USENIX Enigma 2023

DOMINIK WERMKE

Security & Privacy Researcher

CISPA Helmholtz Center for Information Security

dominik.wermke@cispa.de

@sun_grazer



dwermke.com/enigma




THE SUPPLY CHAIN
IS UNDER
ATTACK!



Bleeping Computer

Hundreds of U.S. news sites push malware in supply-chain attack



The threat actor behind this supply-chain attack (tracked by ... employees of more than 30 major U.S. private firms via fake software update...

Bleeping Computer

Hundreds of U.S. news sites push malware in supply chain at

Th

30

TechTarget

Microsoft: Nation-state threats, zero-day attacks increasing

"While zero-day vulnerability attacks tend to initially target a ... the software supply chain to exploiting the IT services supply chain,...



Bleeping Computer

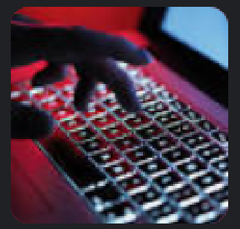
Hundreds of U.S. news sites push malware in supply chain

TechTarget

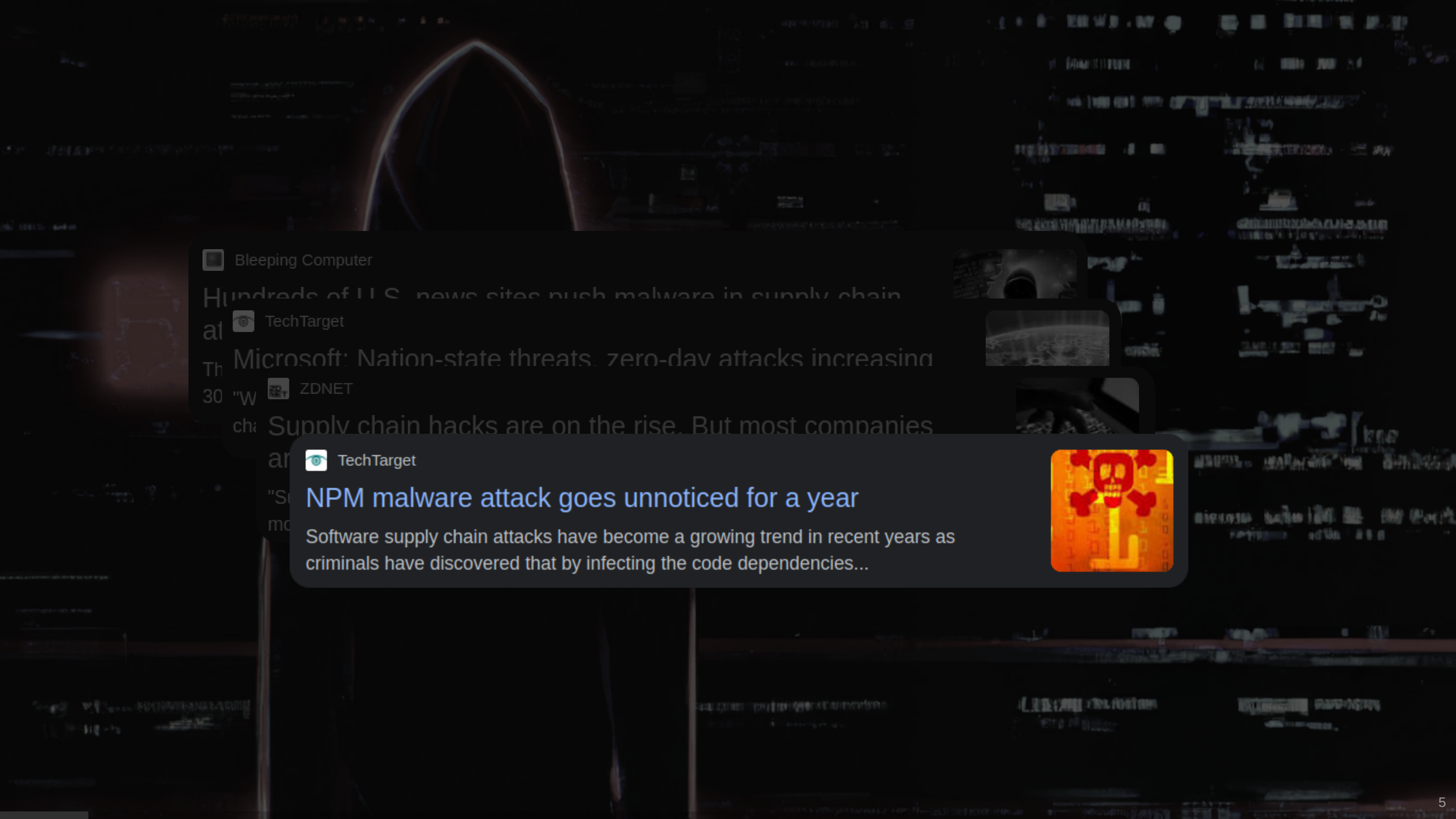
Microsoft: Nation-state threats, zero-day attacks increasing

ZDNET

Supply chain hacks are on the rise. But most companies aren't prepared



"Supply chain attacks are a major cyber threat facing ... US spy agency, the NSA, last month published its software supply chain guidance,...


Bleeping Computer
TechTarget
Microsoft: Nation-state threats, zero-day attacks increasing
ZDNET
TechTarget
NPM malware attack goes unnoticed for a year
Software supply chain attacks have become a growing trend in recent years as criminals have discovered that by infecting the code dependencies...

TARGETING DEVELOPERS



Python developers warned to watch for rogue ‘torchtriton’ package

Hackers logged a fake version of a package used by PyTorch developers that was able to send information to a remote server.

Tech Monitor, 2023-01-03

DEVELOPERS AS THE WEAKEST LINK



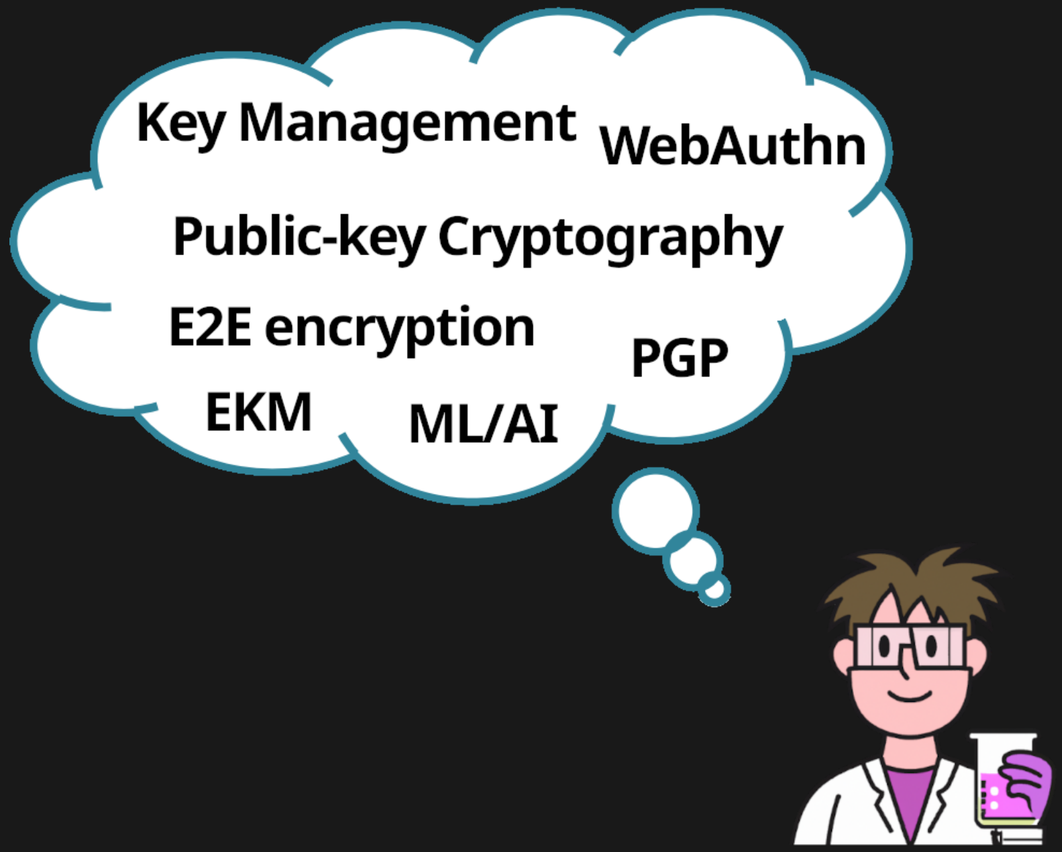
> [A]n unauthorized third party leveraged malware deployed to a CircleCI engineer's laptop in order to steal a valid, 2FA-backed SSO session.

CircleCI

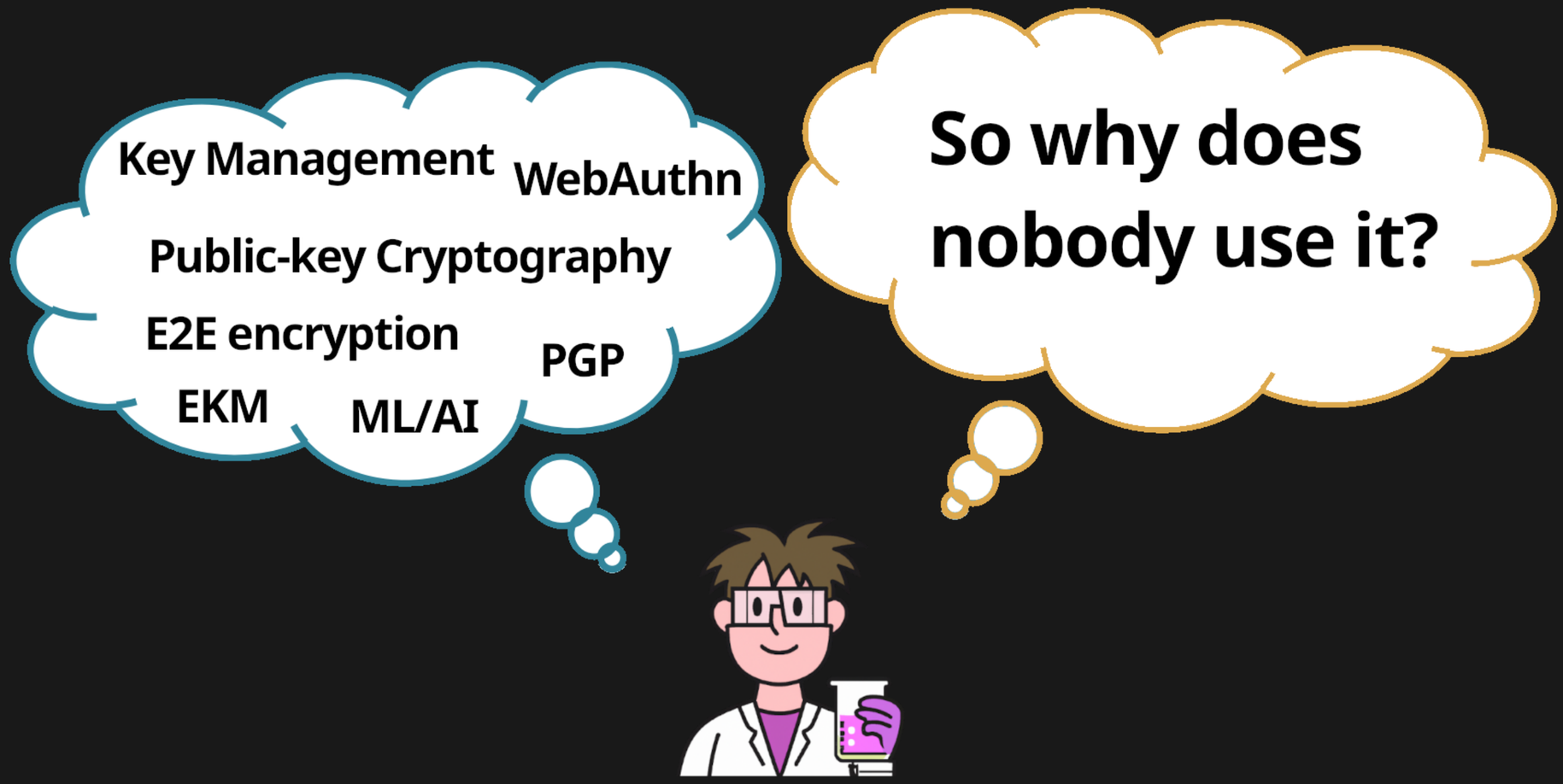
WHERE DOES RESEARCH GET INVOLVED?



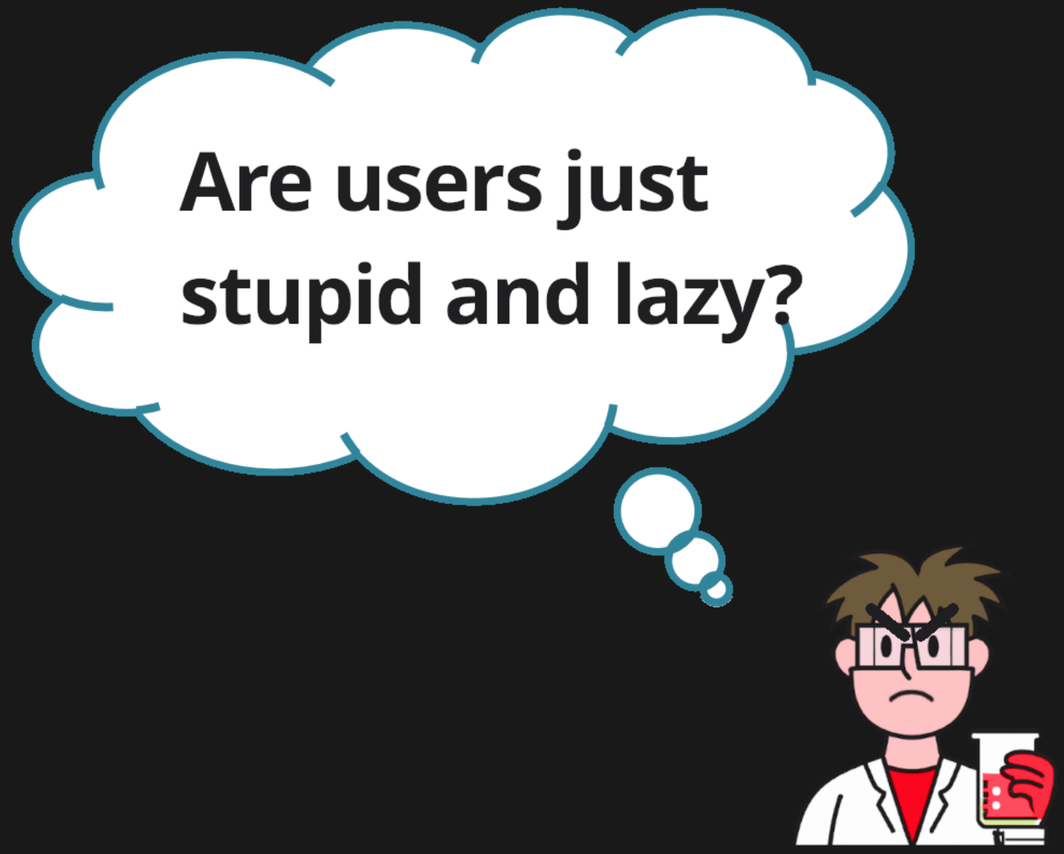
Usable Security & Privacy



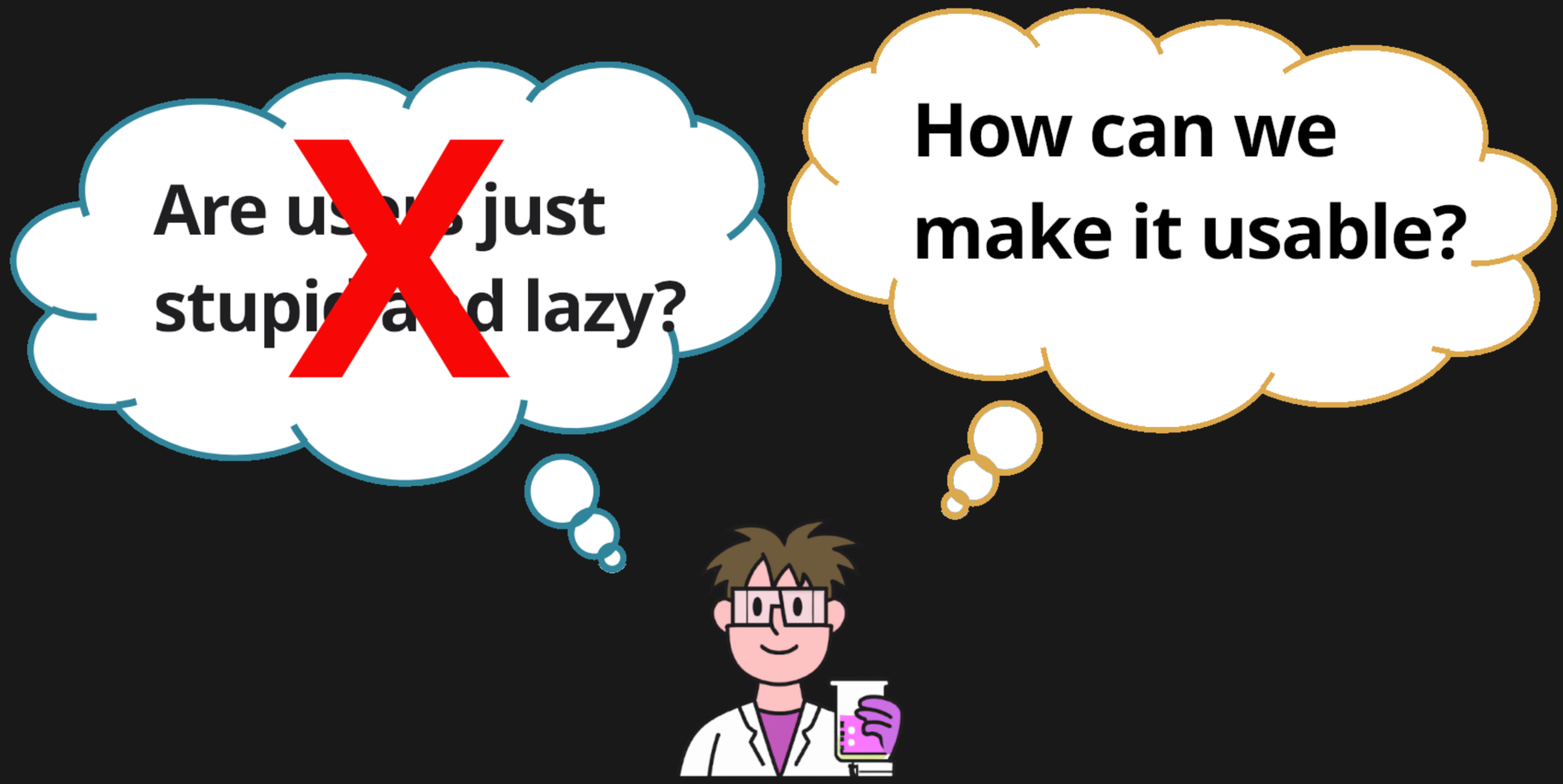
Security & Privacy



Security & Privacy



Security & Privacy



Usable Security & Privacy

If it's not the users fault ...

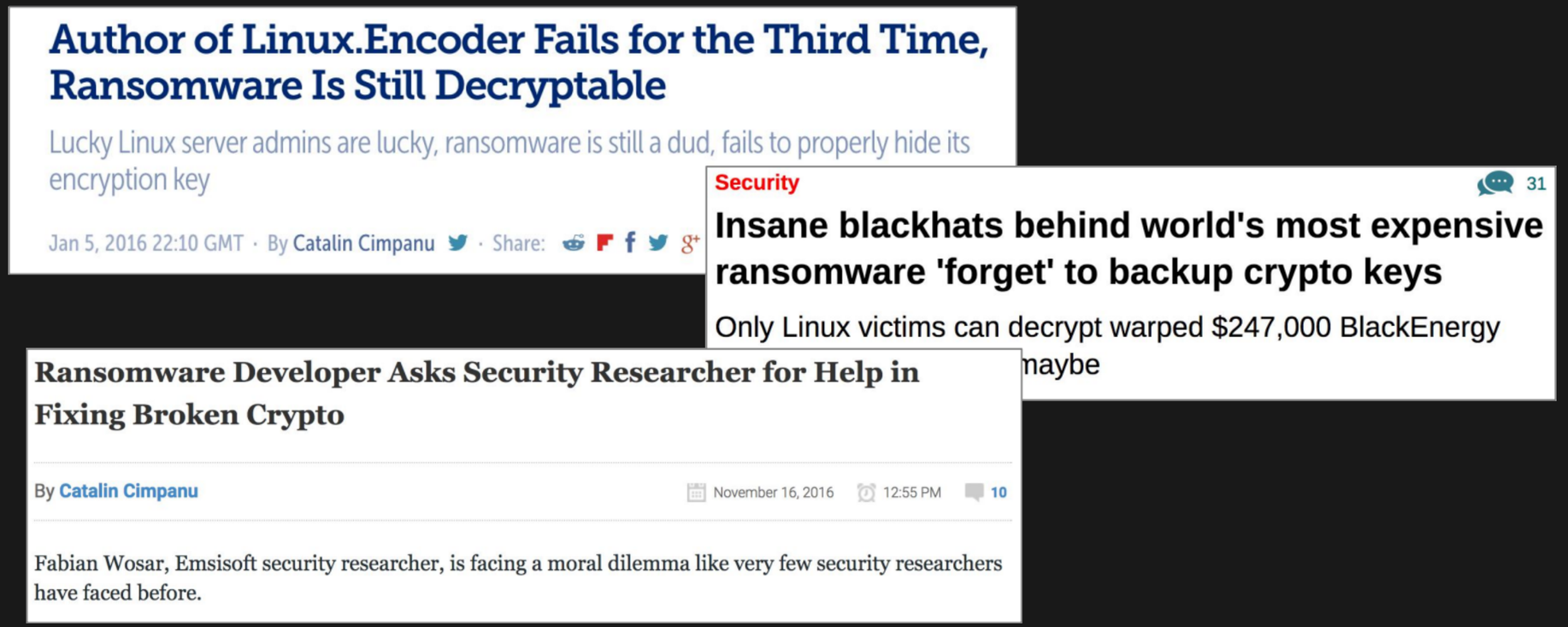
- **Log4Shell** vulnerability
- **Heartbleed**, Cloudbleed
- **Shellshock** vulnerability, Bashdoor

If it's not the users fault ...

- Log4Shell vulnerability
- Heartbleed, Cloudbleed
- Shellshock vulnerability, Bashdoor

... is it the developers fault?

EVEN THE BAD GUYS FAIL



Author of Linux.Encoder Fails for the Third Time, Ransomware Is Still Decryptable

Lucky Linux server admins are lucky, ransomware is still a dud, fails to properly hide its encryption key

Jan 5, 2016 22:10 GMT · By Catalin Cimpanu · Share:

Security 31

Insane blackhats behind world's most expensive ransomware 'forget' to backup crypto keys

Only Linux victims can decrypt warped $247,000 BlackEnergy
maybe

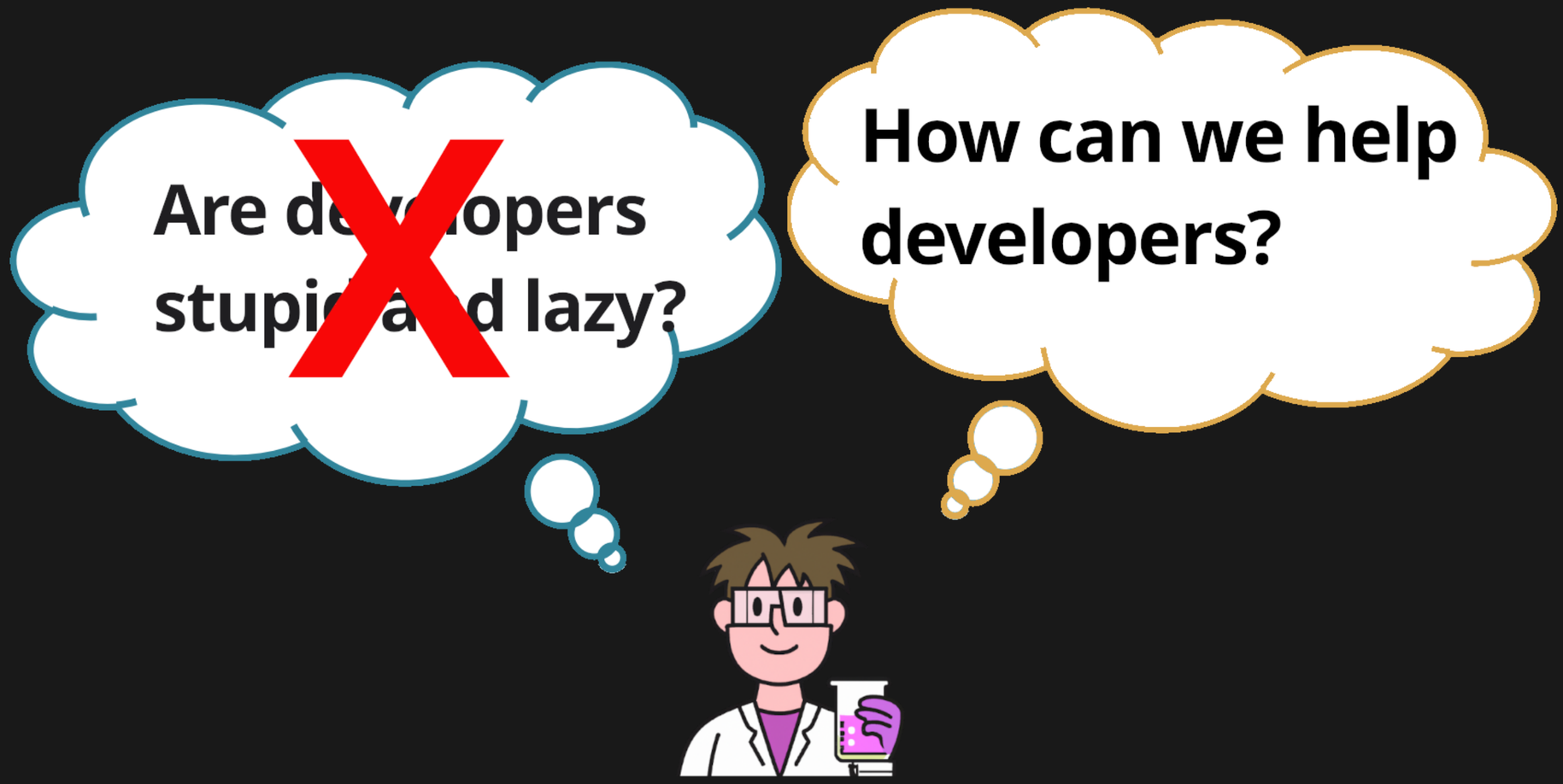
Ransomware Developer Asks Security Researcher for Help in Fixing Broken Crypto

By Catalin Cimpanu November 16, 2016 12:55 PM 10

Fabian Wosar, Emsisoft security researcher, is facing a moral dilemma like very few security researchers have faced before.



Usable Security & Privacy



Usable Security & Privacy for Developers



How can we help ...

- Developers
- Maintainers
- Administrators
- ...

WHY EXPERTS?

WHY EXPERTS?

Users

Administrators

Maintainers

Developers

Project Leads



WHY EXPERTS?

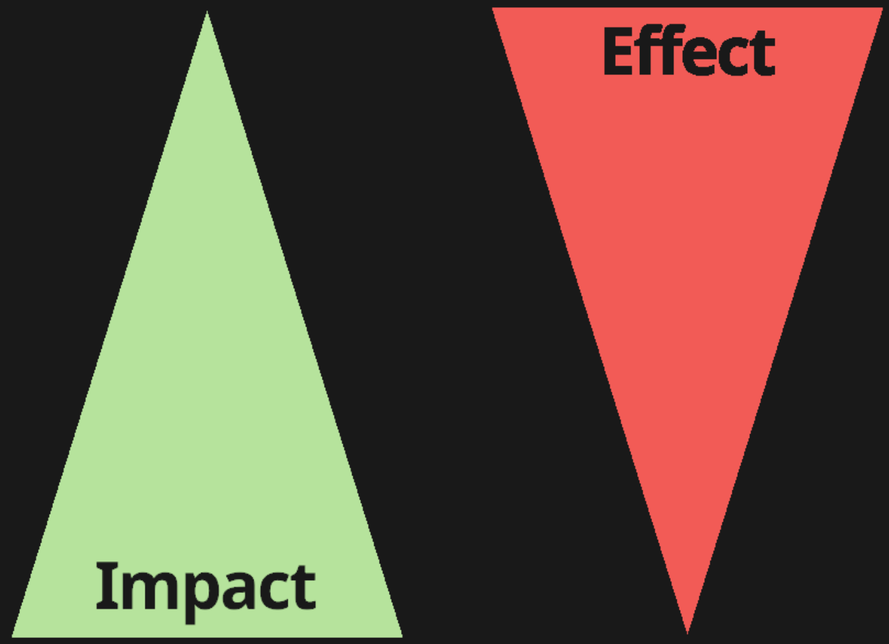
Users

Administrators

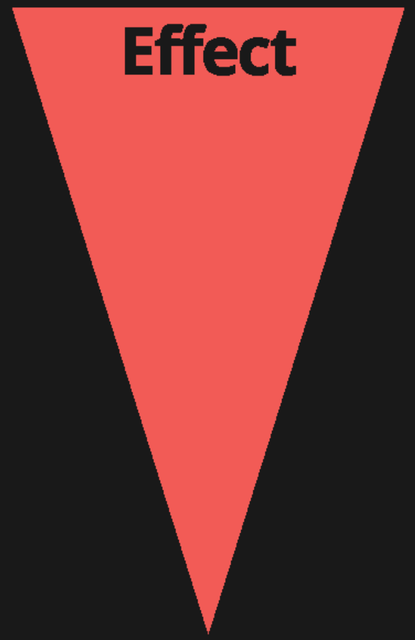
Maintainers

Developers

Project Leads



WHY EXPERTS?



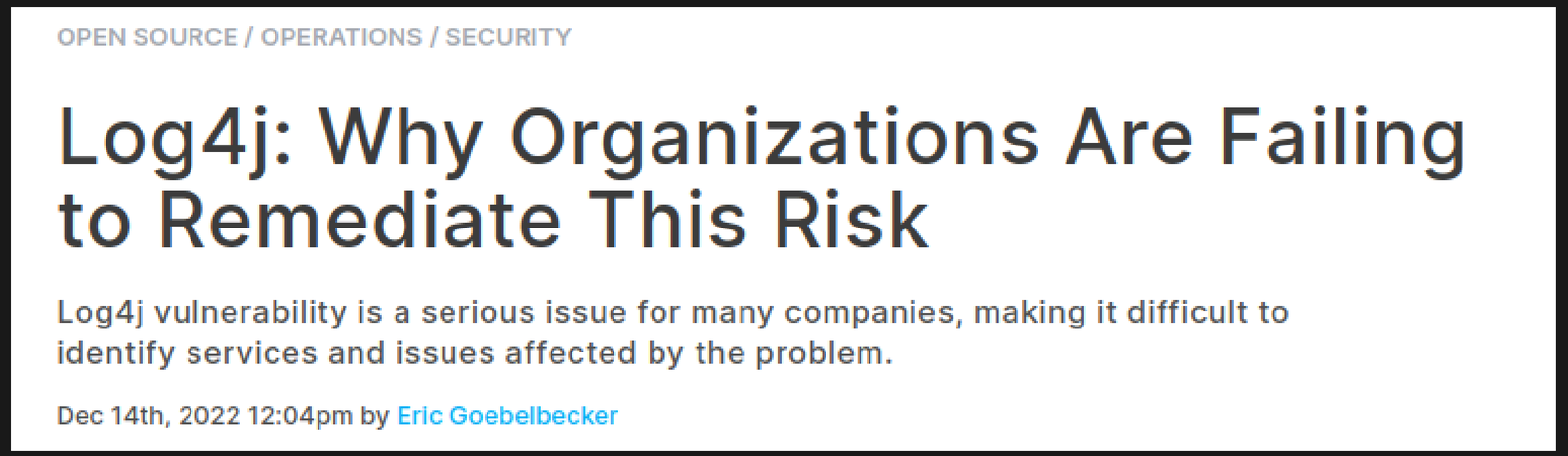
1,000,000s of end users

1000s of deployments

100s of lines of code

10s of projects

EXPERTS BUT NOT SECURITY EXPERTS



OPEN SOURCE / OPERATIONS / SECURITY

Log4j: Why Organizations Are Failing to Remediate This Risk

Log4j vulnerability is a serious issue for many companies, making it difficult to identify services and issues affected by the problem.

Dec 14th, 2022 12:04pm by Eric Goebelbecker

The New Stack

TECHNOLOGY ONLY CAN'T SOLVE THE PROBLEM

TECHNOLOGY ONLY CAN'T SOLVE THE PROBLEM

A Breach at LastPass Has Password Lessons for Us All

The hacking of the password manager should make us reassess whether to trust companies to store our sensitive data in the cloud.

> The company said intruders had gained access to its cloud database and obtained a copy of the data vaults of tens of millions of customers by using credentials and keys stolen from a LastPass employee.

New York Times, 2023-01-05

TECHNOLOGY ONLY CAN'T SOLVE THE PROBLEM

GitHub's Copilot may steer you into dangerous waters about 40% of the time – study

Unless you like shipping buggy or vulnerable code, keep your hands on the wheel

> Given 89 scenarios, about 40 per cent of the computer programs made with the help of Copilot had potentially exploitable vulnerabilities.

The Register

OPEN SOURCE SOFTWARE



Usage: Most projects on their platform rely on some form of Open Source Software

OPEN SOURCE SOFTWARE



Usage: Most projects on their platform rely on some form of Open Source Software

Connected: Median of 683 transitive dependencies in the npm ecosystem

Why you should care about Open Source

OPEN SOURCE SOFTWARE



OPEN SOURCE SUPPLY CHAIN



Open Source code appears as foundation, glue, or during the build process in many software projects.

Committed to Trust: 27 interviews with maintainers of OSS [IEEE S&P 2022]

Reproducible Builds: 24 interviews with reproducible builds stakeholders [Ongoing]

Open Source Components: 25 interviews with company stakeholders using OSS [Ongoing]

COMMITTED TO TRUST

A QUALITATIVE STUDY ON SECURITY & TRUST IN OPEN SOURCE SOFTWARE PROJECTS

Dominik Wermke *
CISPA
dominik.wermke@cispa.de

Noah Wöhler
CISPA
noah.woehler@cispa.de

Jan H. Klemmer
Leibniz University Hannover
klemmer@sec.uni-hannover.de

Marcel Fourné
MPI-SP
marcel.fourne@mpi-sp.org

Yasemin Acar
George Washington University
acar@gwu.edu

Sascha Fahl
CISPA
fahl@cispa.de

RESEARCH QUESTIONS

RESEARCH QUESTIONS

RQ1: How are open source projects structured behind-the-scenes?

RESEARCH QUESTIONS

RQ1: How are open source projects structured behind-the-scenes?

RQ2: If and what guidance and policies are provided by open source projects?

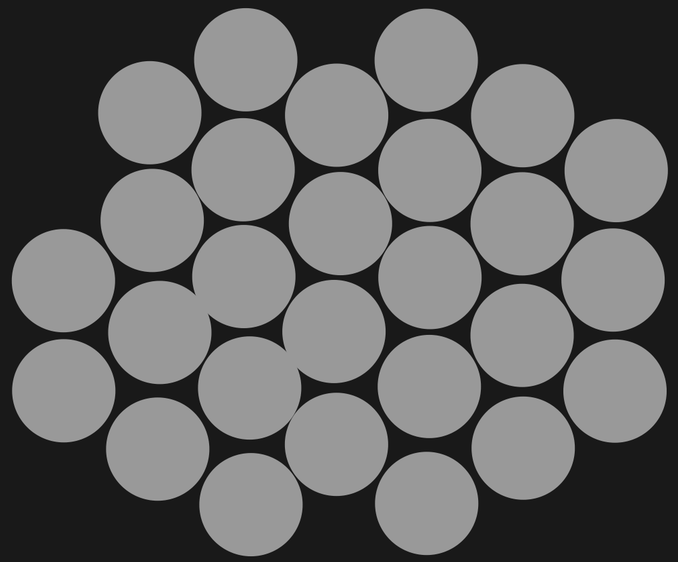
RESEARCH QUESTIONS

RQ1: How are open source projects structured behind-the-scenes?

RQ2: If and what guidance and policies are provided by open source projects?

RQ3: How do open source projects approach security and trust challenges?

INTERVIEWS



INTERVIEWS



Project Leads, Maintainers, Contributors

DEMOGRAPHICS

Highest project role of participants

Contributors - Maintainers - Leaders - Owners

DEMOGRAPHICS

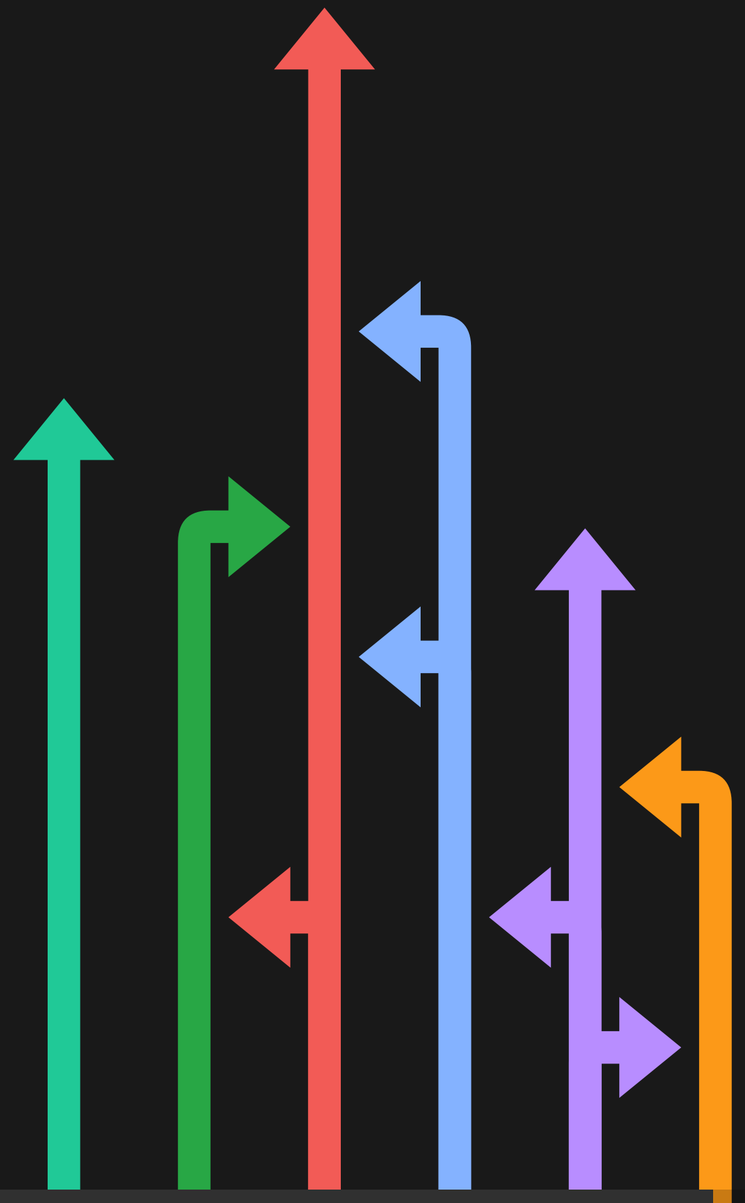
Highest project role of participants

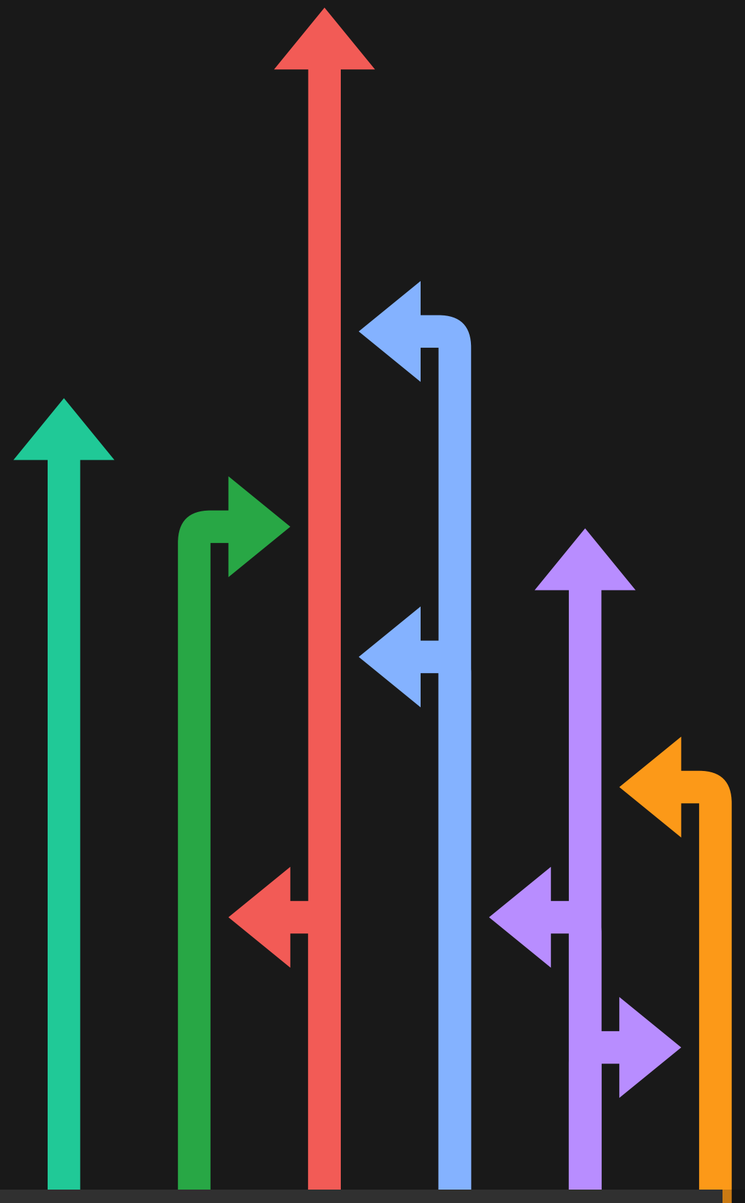


Contributors (4) - Maintainers (3) - Leaders (7) - Owners (9)

Other: 4

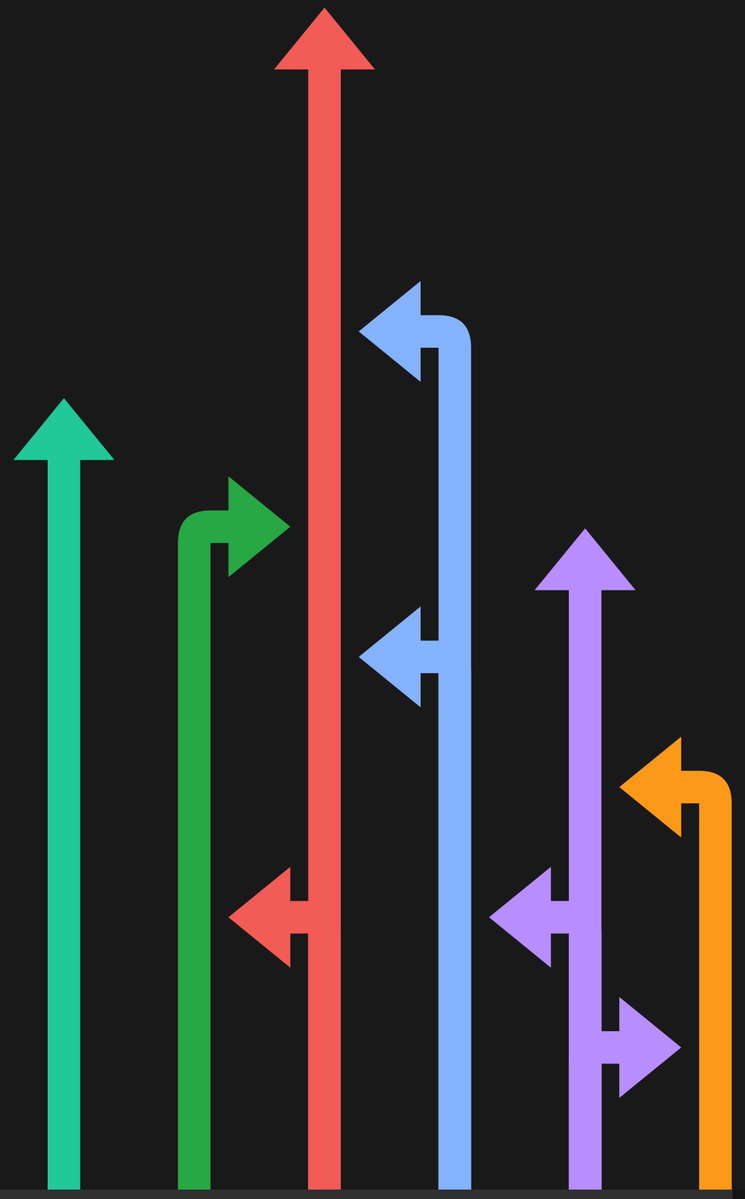
RESULTS





RESULTS

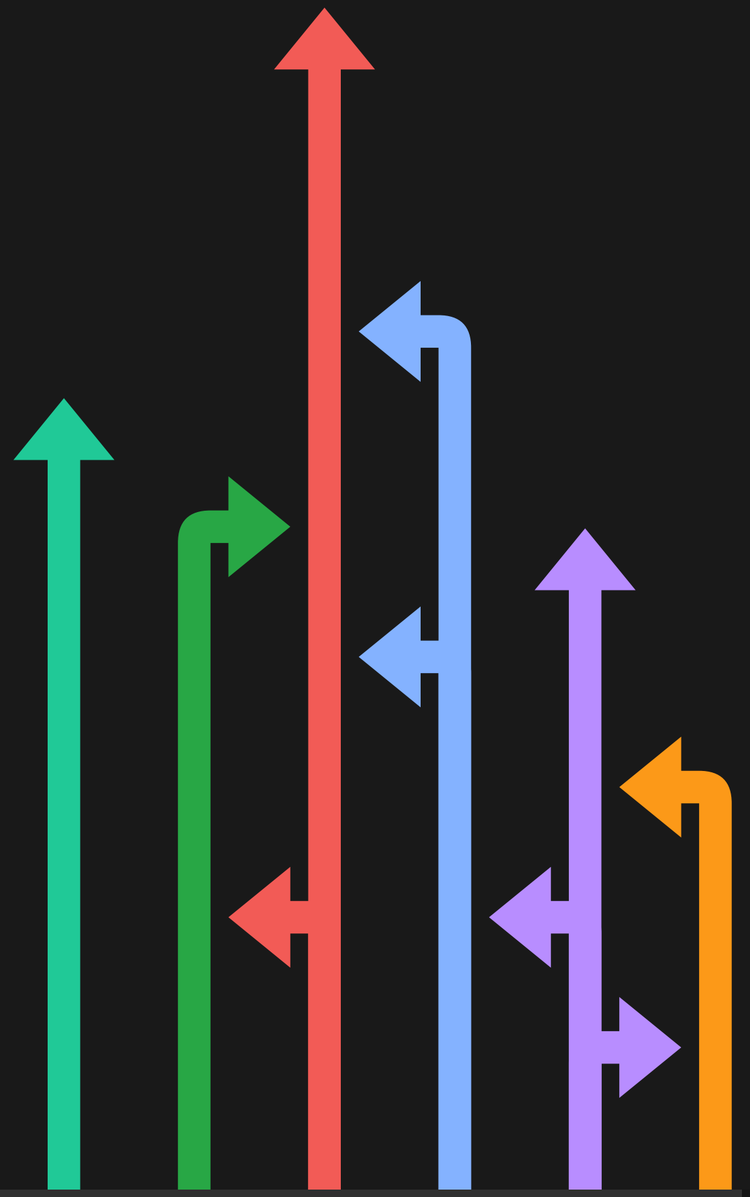
Trust



RESULTS

Trust

Security



RESULTS

Trust

Security

Processes

TRUST

Trust	Security	Processes

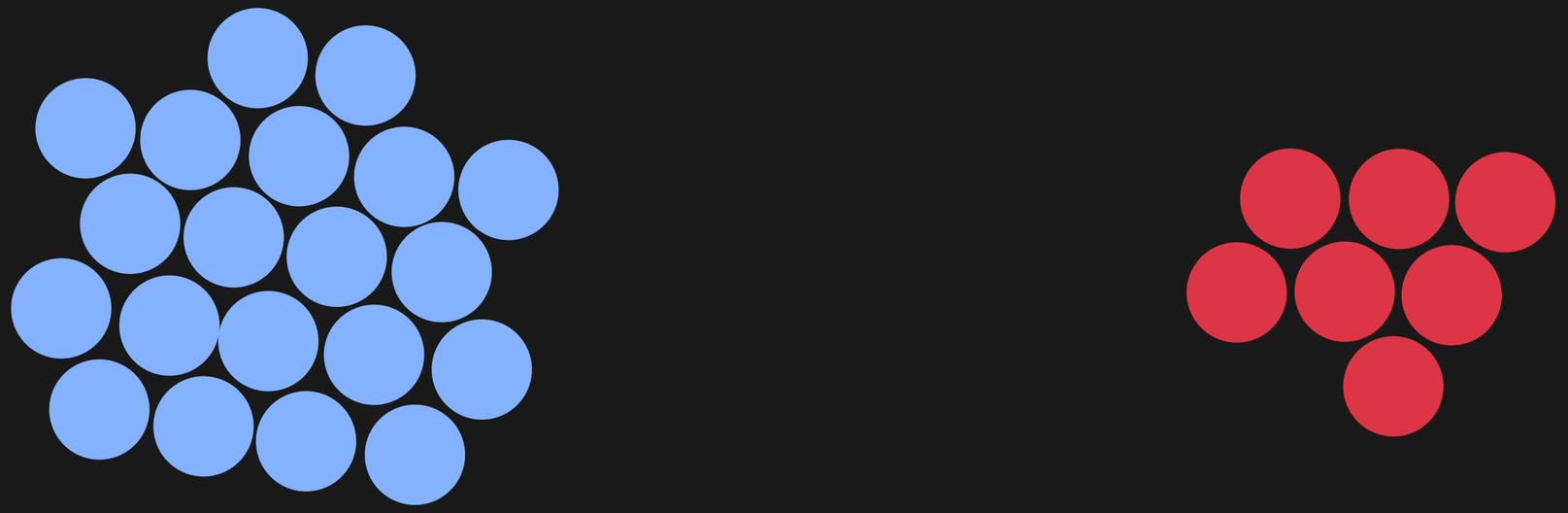
TRUST INCIDENTS

Trust incidents encountered in the past:

None --- Some / Other

TRUST INCIDENTS

Trust incidents encountered in the past:



None (20) --- Some / Other (7)

TRUST INCIDENTS

Trust incidents encountered in the past:

- Drive-by cryptocurrency miner commits
- Failed background checks
- Pro-active block after potential SSH key theft

TRUST PROCESSES

Summary

- Most use some form of meritocracy for establishing trust with new contributors.
- Some even assume trustworthiness by default to facilitate first-time contributions.
- The majority never experienced a trust incident in their projects and did not establish specific trust incident strategies.

SECURITY

Trust | Security | Processes

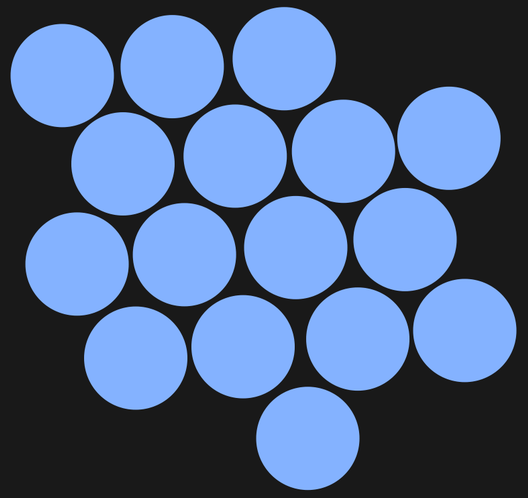
PAST INCIDENTS

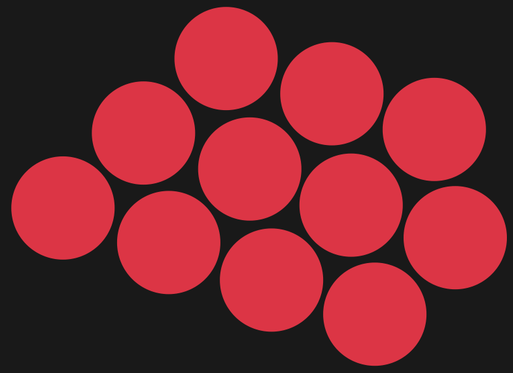
Security incidents encountered in the past:

None --- Some / Other

PAST INCIDENTS

Security incidents encountered in the past:





None (16) --- Some / Other (11)

PAST CHALLENGES

Most commonly encountered security challenges

(That not necessarily resulted in an incident)

- (15) Suspicious or low quality commits
- (8) Vulnerability introduced by dependencies

SECURITY CHALLENGES

Summary

- Few projects have experienced an outright security incident
- Many of our participants were familiar with suspicious or low quality commits and potential vulnerabilities introduced by dependencies

PROCESSES

Trust | Security | Processes

GUIDANCE

Most mentioned guidances

- (14) Guidance for contributing to the project
- (13) Programming language-specific guidance
- (8) General guidance for project setup and infrastructure

GUIDANCE

> Somebody would have to write the guide, and I am the only one who can write it. I mean, there is nobody paid to write it and I am also not paid to write it.

PROCESSES

Summary

- Participants diverge on their opinions regarding the helpfulness of (written) guidance
- Security policies: larger projects mentioned dedicated security teams, smaller projects mentioned a security contact channel
- Most projects included some type of disclosure policy or at least contact for security issues

COMMITTED TO TRUST

Recap

- Projects are highly diverse in deployed security measures, trust processes, and motivations

COMMITTED TO TRUST

Recap

- Projects are highly diverse in deployed security measures, trust processes, and motivations
- Growing scope and contributors → growing needs for security and trust processes

COMMITTED TO TRUST

Recap

- Projects are highly diverse in deployed security measures, trust processes, and motivations
- Growing scope and contributors → growing needs for security and trust processes
- Smaller projects handle security and trust incidents "as they happen"

REPRODUCIBLE BUILDS

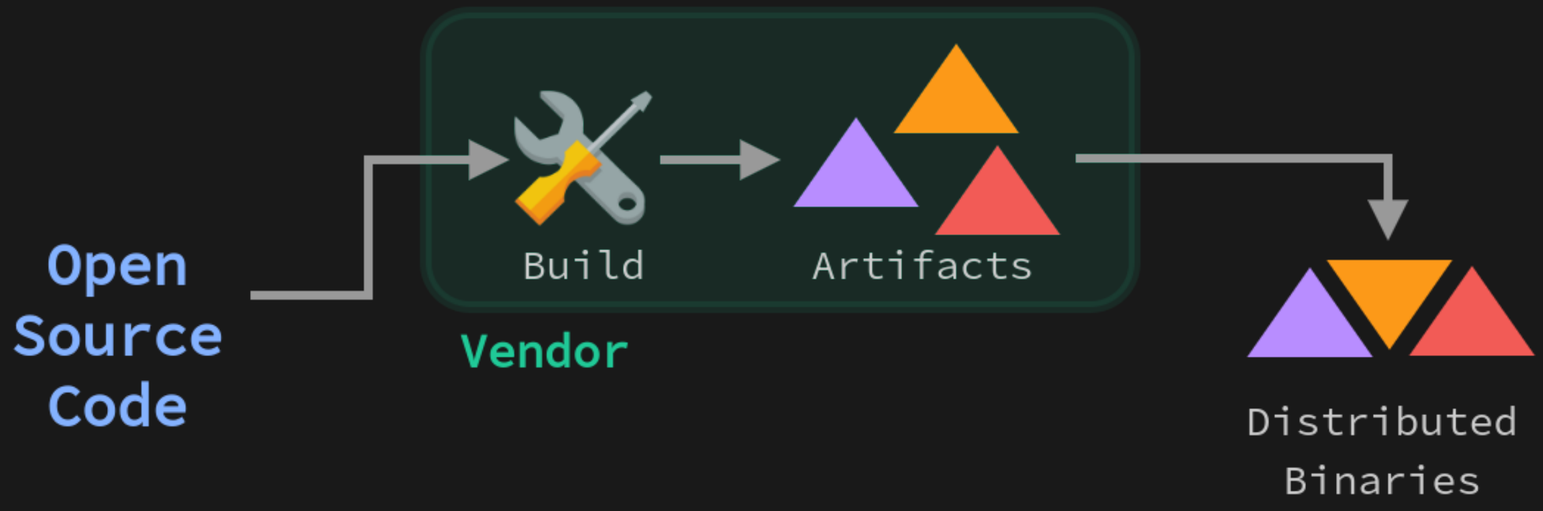


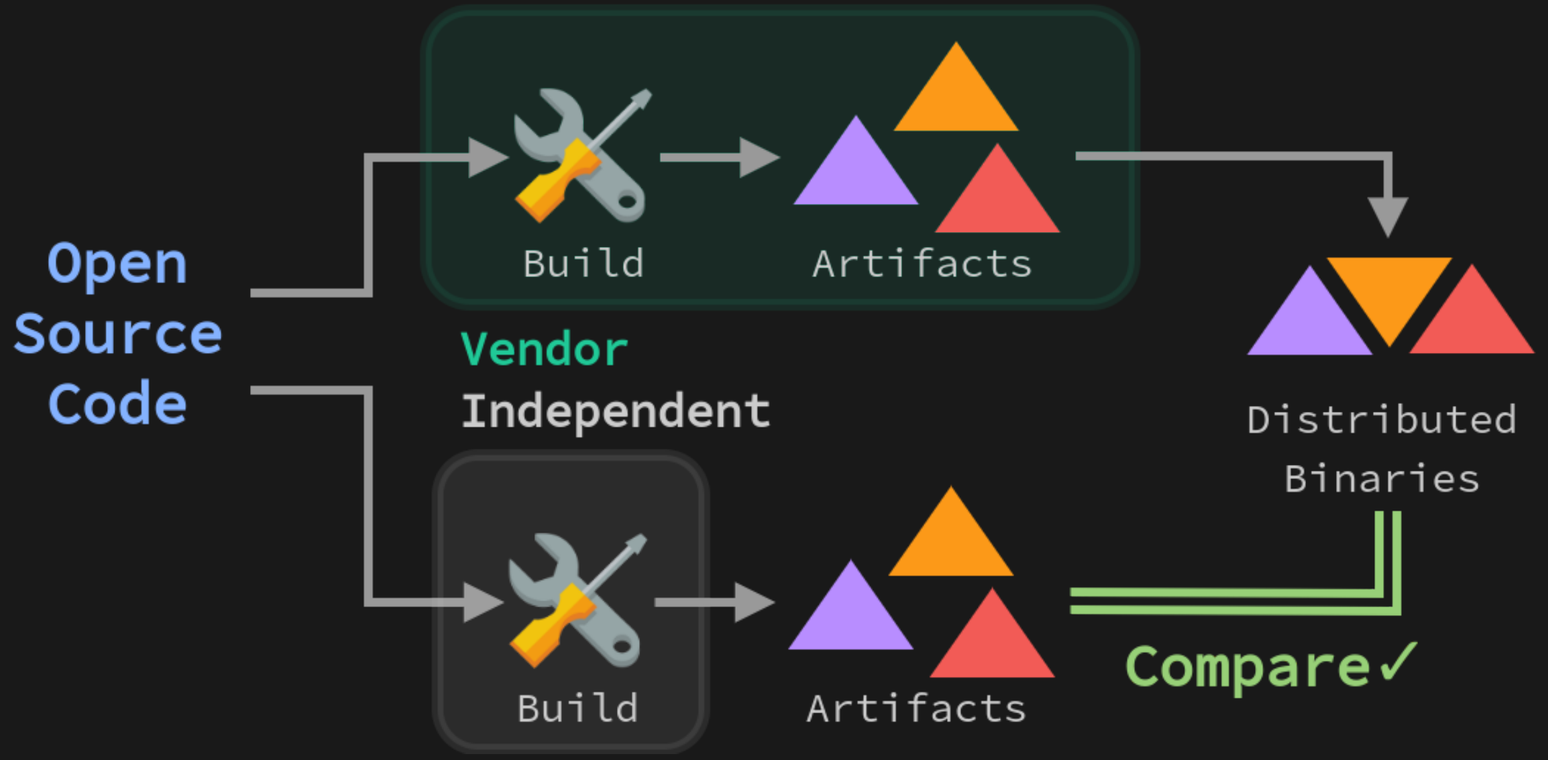
> To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

~ Ken Thompson

REPRODUCIBLE BUILDS

- An important step of trusting the people that wrote the software, is to also be able to trust the resulting artifacts
- Reproducible builds are a solution to this problem

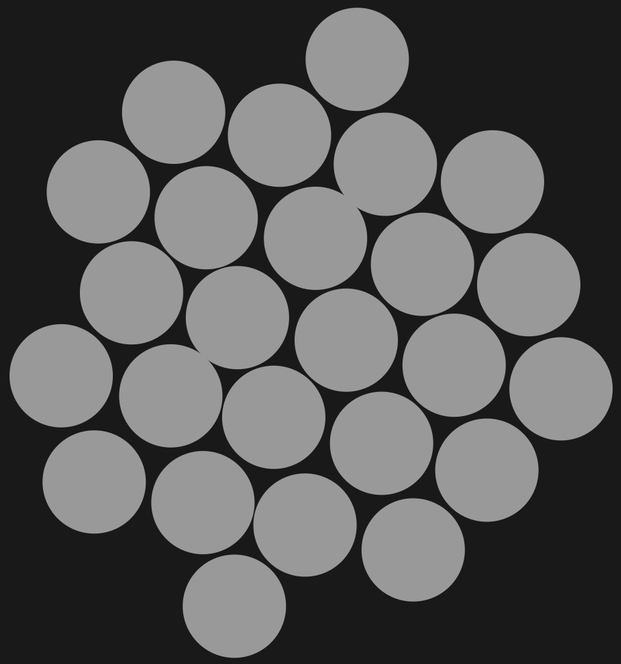

Open
Source
Code
Build
Artifacts
Vendor
Distributed
Binaries


Open
Source
Code
Build
Artifacts
Vendor
Independent
Distributed
Binaries
Build
Artifacts
Compare✓

CHALLENGES

- Timestamps (current)
- File order and build directories
- Any build randomness

INTERVIEWS



INTERVIEWS



Reproducible Builds Experts

PRELIMINARY FINDINGS

- Motivation: "Same input should always compile to same output" and broken expectations

PRELIMINARY FINDINGS

- Experiences: "Receptive upstream projects" and "Patience and Communication"

PRELIMINARY FINDINGS

- Common Obstacles: Date and other times, build directory name inclusion

OPEN SOURCE COMPONENTS IN INDUSTRY

SECURITY CHALLENGES FOR INDUSTRY

- "Other side" of the open source supply chain

SECURITY CHALLENGES FOR INDUSTRY

- "Other side" of the open source supply chain
- How do Industry projects deal with challenges of including open source components?

SECURITY CHALLENGES FOR INDUSTRY

- "Other side" of the open source supply chain
- How do Industry projects deal with challenges of including open source components?
- Investigate their projects' processes, decisions, and considerations

RESEARCH QUESTIONS

RESEARCH QUESTIONS

RQ1: How are Open Source Components included in companies' tech stacks in terms of position, importance, and security effects?

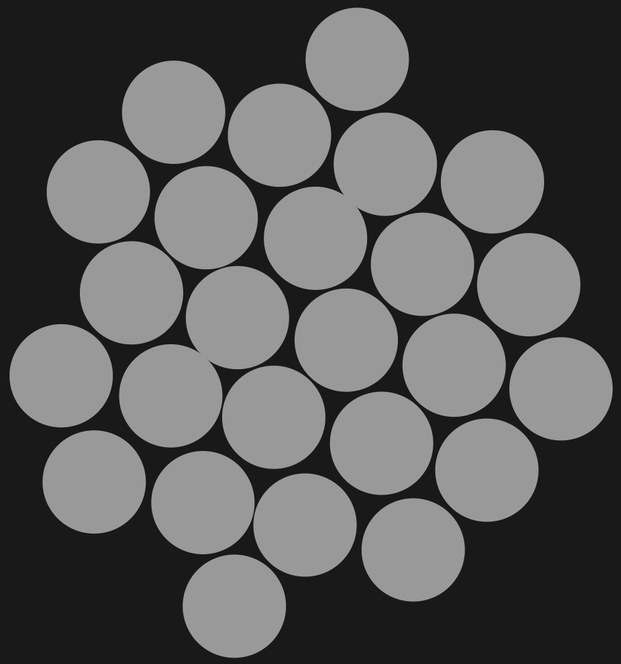
RESEARCH QUESTIONS

RQ2: What are companies' awareness, experiences, and attitudes regarding the security of including external open source code?

RESEARCH QUESTIONS

RQ3: If and how do stakeholders make decisions and considerations around security and trust challenges of including Open Source Components?

INTERVIEWS



INTERVIEWS



Industry Stakeholders

PRELIMINARY FINDINGS

SECURITY CHALLENGES

Projects that encountered security challenge due to OSC

No --- Some / Other

SECURITY CHALLENGES

Projects that encountered security challenge due to OSC



No (1) --- Some / Other (24)

SELECTION CRITERIA

Most common metrics for selecting OS projects

- (16) Popularity measure like downloads or GitHub stars
- (11) Large and active community
- (10) Activity measures like commit frequency and recent releases
- (10) Specific features

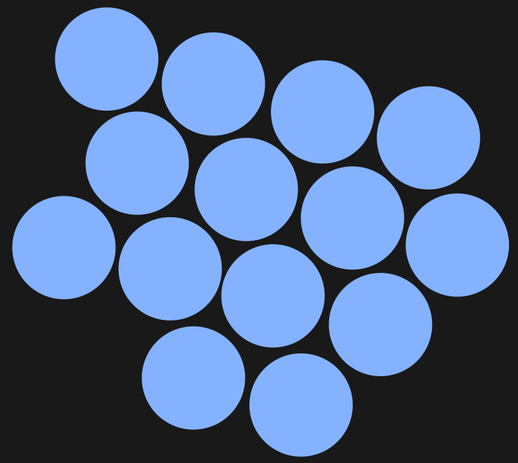
INTERNAL MIRRORS

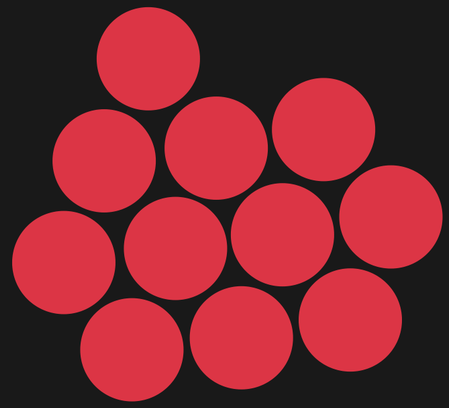
Projets that use (at least partially) internal mirrors:

Yes --- No / Other

INTERNAL MIRRORS

Projets that use (at least partially) internal mirrors:



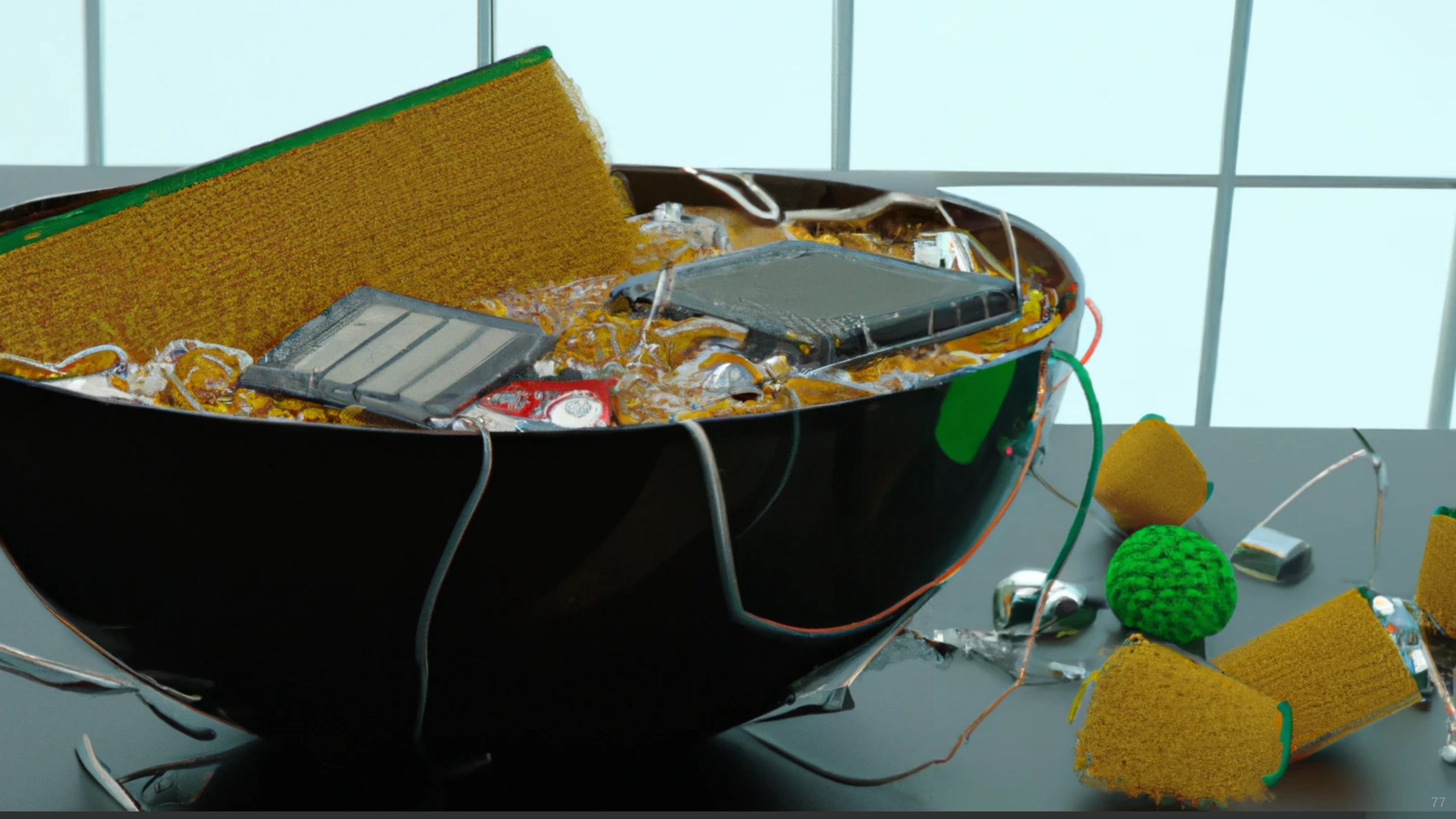


Yes (14) --- No / Other (11)

"NOT YOUR AVERAGE SUPPLY CHAIN"

- Some participants mentioned that their management doesn't seem to fully grasp the benefits and challenges of open source software
- While other support utilized open source components by donating, e.g., money, developer-hours, knowledge, or code
- Few mentioned even following the guideline to "always contribute back"

TAKEAWAYS



SECURING A BOWL OF SPAGHETTI

SECURING A BOWL OF SPAGHETTI

- Software supply chain analogy: (wrongly) conveys linear relations

SECURING A BOWL OF SPAGHETTI

- Software supply chain analogy: (wrongly) conveys linear relations
- With clear start (producer) and end (consumer) endpoints

SECURING A BOWL OF SPAGHETTI

- Software supply chain analogy: (wrongly) conveys linear relations
- With clear start (producer) and end (consumer) endpoints
- In reality: a giant bowl of spaghetti

SECURING A BOWL OF SPAGHETTI

- Software supply chain analogy: (wrongly) conveys linear relations
- With clear start (producer) and end (consumer) endpoints
- In reality: a giant bowl of spaghetti
- Some companies focus on stuff on their plate

Committed to Trust: 27 interviews with maintainers of OSS [IEEE S&P 2022]

Reproducible Builds: 24 interviews with reproducible builds stakeholders [Ongoing]

Open Source Components: 25 interviews with company stakeholders using OSS [Ongoing]

TAKEAWAYS

Open Source: Not your average supply chain

TAKEAWAYS

Open Source: Not your average supply chain

Developers: Weakest link in the software supply chain

TAKEAWAYS

Open Source:	Not your average supply chain
Developers:	Weakest link in the software supply chain
Solution:	Involve the developers!

UNDERSTANDING TRUST AND SECURITY PROCESSES IN THE OPEN SOURCE SOFTWARE ECOSYSTEM

dwermke.com/enigma

Committed to Trust: A Qualitative Study on Security & Trust in Open Source Software Projects
Wermke et al., *IEEE S&P 2022*.

Reproducible Builds
[Ongoing]

Open Source Components in Industry Projects
[Ongoing]

SOCIALS

Dominik Wermke (dwermke.com)
dominik.wermke@cispa.de
@sun_grazer



Understanding Trust and Security Processes in the Open Source Software Ecosystem

Dominik Wermke
dwermke.com/enigma

USENIX Enigma 2023