

# Never Mind the Checkboxes, Here's Reproducible Builds!

Vagrant Cascadian & Chris Lamb

FOSSY 2025-08-02



# Who we are



We are a small part of the Reproducible Builds community, which now comprises over around 300 contributors and 40 separate software projects. Although the idea is an old one, we were motivated to start our project after a series of global surveillance disclosures in the mid-2010s.

# What the punk

A selection of Punk values

- ...

# What the punk

A selection of Punk values

- ...
- Autonomy

# What the punk

A selection of Punk values

- ...
- Autonomy
- Independence

# What the punk

A selection of Punk values

- ...
- Autonomy
- Independence
- Mutual Aid

# What the punk

## A selection of Punk values

- ...
- Autonomy
- Independence
- Mutual Aid
- Community



# What the punk

## A selection of Punk values

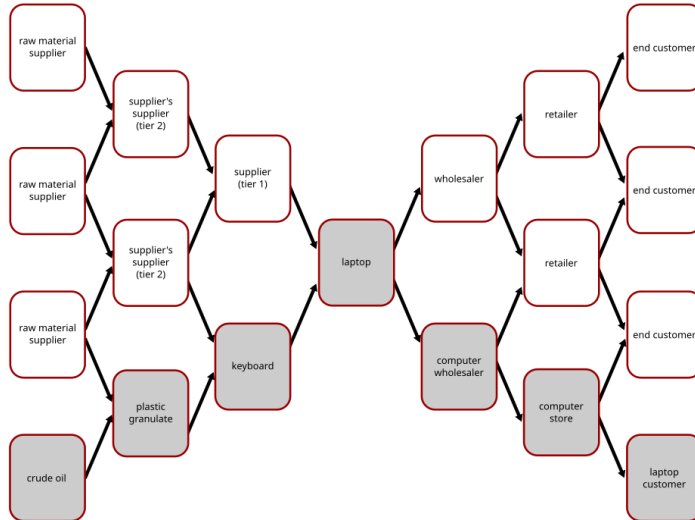
- ...
- Autonomy
- Independence
- Mutual Aid
- Community
- DIY

# What the punk

A selection of Punk values

- ...
- Autonomy
- Independence
- Mutual Aid
- Community
- DIY
- Blatant Disregard for Authority

# Physical Supply chains



# Chained to your Supply

[https://en.wikipedia.org/wiki/Software\\_supply\\_chain](https://en.wikipedia.org/wiki/Software_supply_chain)

A software supply chain is the components, libraries, tools, and processes used to develop, build, and publish a software artifact.

# Straining the Supply Chain Anology

A software supply chain differs from a physical supply chain in several key ways, which lead to distinct challenges and strategies:

- Software is **intangible**, nearly infinitely and instantaneously duplicated and transmitted
- Software is distributed digitally, allowing instant global reach.
- Different **regulatory environments**
- Software has a different **lifecycle**; it can be technically be updated indefinitely
- Software relies on digital **infrastructure**
- Food and other physical objects require physical transportation
- Hardware or food often has a limited shelf life
- Physical goods require manufacturing and logistical facilities

`https://en.wikipedia.org/wiki/Bill\_of\_materials`

A Bill of Materials (BOM) ... is a list of the raw materials, sub-assemblies, intermediate assemblies, sub-components, parts, and the quantities of each needed to manufacture an end product.

[https://en.wikipedia.org/wiki/Software\\_supply\\_chain](https://en.wikipedia.org/wiki/Software_supply_chain)

A Software Bill of Materials (SBOM) declares the inventory of components used to build a software artifact, including any open source and proprietary software components. It is the software analogue to the traditional manufacturing BOM, which is used as part of supply chain management.

[https://en.wikipedia.org/wiki/ISO\\_9000\\_family](https://en.wikipedia.org/wiki/ISO_9000_family)

The goal of these standards is to help organizations ensure that they meet customer and other stakeholder needs within the statutory and regulatory requirements related to a product or service.

- 1987



[https://en.wikipedia.org/wiki/ISO\\_9000\\_family](https://en.wikipedia.org/wiki/ISO_9000_family)

The goal of these standards is to help organizations ensure that they meet customer and other stakeholder needs within the statutory and regulatory requirements related to a product or service.

- 1987
- International

[https://en.wikipedia.org/wiki/ISO\\_9000\\_family](https://en.wikipedia.org/wiki/ISO_9000_family)

The goal of these standards is to help organizations ensure that they meet customer and other stakeholder needs within the statutory and regulatory requirements related to a product or service.

- 1987
- International
- third-party certification

[https://en.wikipedia.org/wiki/Cyber\\_Resilience\\_Act](https://en.wikipedia.org/wiki/Cyber_Resilience_Act)

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202402847](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847)

- 2024

[https://en.wikipedia.org/wiki/Cyber\\_Resilience\\_Act](https://en.wikipedia.org/wiki/Cyber_Resilience_Act)

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202402847](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847)

- 2024
- Europe

[https://en.wikipedia.org/wiki/Cyber\\_Resilience\\_Act](https://en.wikipedia.org/wiki/Cyber_Resilience_Act)

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202402847](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847)

- 2024
- Europe
- Voluntary self assessment

[https://en.wikipedia.org/wiki/Cyber\\_Resilience\\_Act](https://en.wikipedia.org/wiki/Cyber_Resilience_Act)

[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202402847](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847)

- 2024
- Europe
- Voluntary self assessment
- Open Source Stewards

# Executively Ordered

<https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

Whitehouse Executive Order 14028

Improving the Nation's Cybersecurity

- 2021

<https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

Whitehouse Executive Order 14028

Improving the Nation's Cybersecurity

- 2021
- United States of America



<https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

Whitehouse Executive Order 14028

Improving the Nation's Cybersecurity

- 2021
- United States of America
- SolarWinds and other big incidents

<https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

Whitehouse Executive Order 14028

Improving the Nation's Cybersecurity

- 2021
- United States of America
- SolarWinds and other big incidents
- Not yet rescinded

<https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

Whitehouse Executive Order 14028

Improving the Nation's Cybersecurity

- 2021
- United States of America
- SolarWinds and other big incidents
- Not yet rescinded
- SBOMs!

<https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

Whitehouse Executive Order 14028

Improving the Nation's Cybersecurity

- 2021
- United States of America
- SolarWinds and other big incidents
- Not yet rescinded
- SBOMs!
- autogenerated SBOMs

<https://openchainproject.org/checklist-iso-dis-18974>

- ...

<https://openchainproject.org/checklist-iso-dis-18974>

- ...
- Voluntary self assessment

<https://openchainproject.org/checklist-iso-dis-18974>

- ...
- Voluntary self assessment
- We have security policies

<https://openchainproject.org/checklist-iso-dis-18974>

- ...
- Voluntary self assessment
- We have security policies
- We have people



<https://openchainproject.org/checklist-iso-dis-18974>

- ...
- Voluntary self assessment
- We have security policies
- We have people
- Who know about the policies

<https://openchainproject.org/checklist-iso-dis-18974>

- ...
- Voluntary self assessment
- We have security policies
- We have people
- Who know about the policies
- We document and review policies

<https://openchainproject.org/checklist-iso-dis-18974>

- ...
- Voluntary self assessment
- We have security policies
- We have people
- Who know about the policies
- We document and review policies
- We document and review implementation of policies

<https://openchainproject.org/checklist-iso-dis-18974>

- ...
- Voluntary self assessment
- We have security policies
- We have people
- Who know about the policies
- We document and review policies
- We document and review implementation of policies
- Security stuff ... (more later)

<https://openchainproject.org/checklist-iso-dis-18974>

- ...
- Voluntary self assessment
- We have security policies
- We have people
- Who know about the policies
- We document and review policies
- We document and review implementation of policies
- Security stuff ... (more later)
- We keep track of our software

<https://openchainproject.org/checklist-iso-dis-18974>

- ...
- Voluntary self assessment
- We have security policies
- We have people
- Who know about the policies
- We document and review policies
- We document and review implementation of policies
- Security stuff ... (more later)
- We keep track of our software
- We archive our software

<https://openchainproject.org/checklist-iso-dis-18974>

- ...
- Voluntary self assessment
- We have security policies
- We have people
- Who know about the policies
- We document and review policies
- We document and review implementation of policies
- Security stuff ... (more later)
- We keep track of our software
- We archive our software
- Document all of the above

<https://openchainproject.org/checklist-iso-dis-18974>

- ...
- Voluntary self assessment
- We have security policies
- We have people
- Who know about the policies
- We document and review policies
- We document and review implementation of policies
- Security stuff ... (more later)
- We keep track of our software
- We archive our software
- Document all of the above
- Review all of the above



# OpenChain: The Security Stuff

<https://openchainproject.org/checklist-iso-dis-18974>

Security Stuff

- Identify threats

# OpenChain: The Security Stuff

<https://openchainproject.org/checklist-iso-dis-18974>

Security Stuff

- Identify threats
- Vulnerability Detection

# OpenChain: The Security Stuff

<https://openchainproject.org/checklist-iso-dis-18974>

## Security Stuff

- Identify threats
- Vulnerability Detection
- Vulnerability follow-up

<https://openchainproject.org/checklist-iso-dis-18974>

## Security Stuff

- Identify threats
- Vulnerability Detection
- Vulnerability follow-up
- Vulnerability communication

# OpenChain: The Security Stuff

<https://openchainproject.org/checklist-iso-dis-18974>

## Security Stuff

- Identify threats
- Vulnerability Detection
- Vulnerability follow-up
- Vulnerability communication
- We test released software

While SBOMs, ISO9660 and other regulatory processes provide a framework standards to enhance security, they fall short of solving real-world security problems.

- They primarily focus on documentation and standardization rather than addressing dynamic and evolving threats

While SBOMs, ISO9660 and other regulatory processes provide a framework standards to enhance security, they fall short of solving real-world security problems.

- They primarily focus on documentation and standardization rather than addressing dynamic and evolving threats
- Static nature of standards (eg. ISO9660) cannot keep pace with the rapid development of vulnerabilities

While SBOMs, ISO9660 and other regulatory processes provide a framework standards to enhance security, they fall short of solving real-world security problems.

- They primarily focus on documentation and standardization rather than addressing dynamic and evolving threats
- Static nature of standards (eg. ISO9660) cannot keep pace with the rapid development of vulnerabilities
- Implementing regulatory processes can be resource-intensive



While SBOMs, ISO9660 and other regulatory processes provide a framework standards to enhance security, they fall short of solving real-world security problems.

- They primarily focus on documentation and standardization rather than addressing dynamic and evolving threats
- Static nature of standards (eg. ISO9660) cannot keep pace with the rapid development of vulnerabilities
- Implementing regulatory processes can be resource-intensive
- Compliance with standards doesn't guarantee overall security resilience, as these frameworks often fail to account for human factors

Does it improve the quality of software?

Do Software Bill of Materials (SBOMs) actually give you the information necessary to verify how a given software artifact was built?

While SBOMs provide valuable information about the components of software, reproducible builds offers a more robust guarantee by directly tying the binary back to the source code. They ensure the actual code can be audited and verified for consistency with the distributed binary, reducing potential vectors for compromise that occur between source code and final product. They therefore provide stronger assurances of integrity and security.

- ...

Do Software Bill of Materials (SBOMs) actually give you the information necessary to verify how a given software artifact was built?

While SBOMs provide valuable information about the components of software, reproducible builds offers a more robust guarantee by directly tying the binary back to the source code. They ensure the actual code can be audited and verified for consistency with the distributed binary, reducing potential vectors for compromise that occur between source code and final product. They therefore provide stronger assurances of integrity and security.

- ...
- list of software dependencies

Do Software Bill of Materials (SBOMs) actually give you the information necessary to verify how a given software artifact was built?

While SBOMs provide valuable information about the components of software, reproducible builds offers a more robust guarantee by directly tying the binary back to the source code. They ensure the actual code can be audited and verified for consistency with the distributed binary, reducing potential vectors for compromise that occur between source code and final product. They therefore provide stronger assurances of integrity and security.

- ...
- list of software dependencies
- may be obfuscated!!!

Do Software Bill of Materials (SBOMs) actually give you the information necessary to verify how a given software artifact was built?

While SBOMs provide valuable information about the components of software, reproducible builds offers a more robust guarantee by directly tying the binary back to the source code. They ensure the actual code can be audited and verified for consistency with the distributed binary, reducing potential vectors for compromise that occur between source code and final product. They therefore provide stronger assurances of integrity and security.

- ...
- list of software dependencies
- may be obfuscated!!!
- may not even be publicly available

What is the goal of all these compliance checklists anyways. . . or more importantly, what should the goals be?

If a software object is signed, who should be trusted to sign it, and can they be trusted ... forever?



# Reproducible Builds Defined

<https://reproducible-builds.org/docs/definition/>

A build is reproducible if, given the same source code, build environment and build instructions, any party can recreate bit-by-bit identical copies of all specified artifacts.



# Why Reproducible Builds Matters

## Why Reproducible Builds Matters

- The crucial reason we care about bit-for-bit Reproducibility, is that if multiple people can all build the same, bit-for-bit, identical copy of the software, then that is pretty strong evidence that none of those builds have been tampered with, and none of those people have been hacked.

# Why Reproducible Builds Matters

## Why Reproducible Builds Matters

- The crucial reason we care about bit-for-bit Reproducibility, is that if multiple people can all build the same, bit-for-bit, identical copy of the software, then that is pretty strong evidence that none of those builds have been tampered with, and none of those people have been hacked.
- This, in turn, then allows other people to trust those builds and install that software on their machines, without building the software themselves.

# Why Reproducible Builds Matters

## Why Reproducible Builds Matters

- The crucial reason we care about bit-for-bit Reproducibility, is that if multiple people can all build the same, bit-for-bit, identical copy of the software, then that is pretty strong evidence that none of those builds have been tampered with, and none of those people have been hacked.
- This, in turn, then allows other people to trust those builds and install that software on their machines, without building the software themselves.
- For example, if I can build exactly what the Debian build servers are building, that is evidence that they have not yet been hacked. Centralised build servers are, of course, very juicy targets for malicious actors.

# What is needed for Reproducible Builds

A build is reproducible if given the same source code, build environment and build instructions, any party can recreate bit-by-bit identical copies of all specified artifacts.

- ...

# What is needed for Reproducible Builds

A build is reproducible if given the same source code, build environment and build instructions, any party can recreate bit-by-bit identical copies of all specified artifacts.

- ...
- Source Code

# What is needed for Reproducible Builds

A build is reproducible if given the same source code, build environment and build instructions, any party can recreate bit-by-bit identical copies of all specified artifacts.

- ...
- Source Code
- Software used during build (build environment)

# What is needed for Reproducible Builds

A build is reproducible if given the same source code, build environment and build instructions, any party can recreate bit-by-bit identical copies of all specified artifacts.

- ...
- Source Code
- Software used during build (build environment)
- Instructions on how to perform the build



# What is needed for Reproducible Builds

A build is reproducible if given the same source code, build environment and build instructions, any party can recreate bit-by-bit identical copies of all specified artifacts.

- ...
- Source Code
- Software used during build (build environment)
- Instructions on how to perform the build
- Any party (e.g. any third party)

# Have I heard this before

Requirements for Reproducible Builds and Free and Open Source Software overlap!

- Source Code

# Have I heard this before

Requirements for Reproducible Builds and Free and Open Source Software overlap!

- Source Code
- Software used during build (build environment)

# Have I heard this before

Requirements for Reproducible Builds and Free and Open Source Software overlap!

- Source Code
- Software used during build (build environment)
- Instructions on how to perform the build

# Have I heard this before

Requirements for Reproducible Builds and Free and Open Source Software overlap!

- Source Code
- Software used during build (build environment)
- Instructions on how to perform the build
- Any party (e.g. any third party)

# Have I heard this before

Requirements for Reproducible Builds and Free and Open Source Software overlap!

- Source Code
- Software used during build (build environment)
- Instructions on how to perform the build
- Any party (e.g. any third party)
- Use

# Have I heard this before

Requirements for Reproducible Builds and Free and Open Source Software overlap!

- Source Code
- Software used during build (build environment)
- Instructions on how to perform the build
- Any party (e.g. any third party)
- Use
- Share

# Have I heard this before

Requirements for Reproducible Builds and Free and Open Source Software overlap!

- Source Code
- Software used during build (build environment)
- Instructions on how to perform the build
- Any party (e.g. any third party)
- Use
- Share
- Study (Source)



# Have I heard this before

Requirements for Reproducible Builds and Free and Open Source Software overlap!

- Source Code
- Software used during build (build environment)
- Instructions on how to perform the build
- Any party (e.g. any third party)
- Use
- Share
- Study (Source)
- Change (Source)

## Reproducible builds of Free and Open Source Software

- ...

# Reproducible Builds

## Reproducible builds of Free and Open Source Software

- ...
- Autonomy and Independence

## Reproducible builds of Free and Open Source Software

- ...
- Autonomy and Independence
- Mutual Aid

## Reproducible builds of Free and Open Source Software

- ...
- Autonomy and Independence
- Mutual Aid
- DIY

## Reproducible builds of Free and Open Source Software

- ...
- Autonomy and Independence
- Mutual Aid
- DIY
- Community

## Reproducible builds of Free and Open Source Software

- ...
- Autonomy and Independence
- Mutual Aid
- DIY
- Community
- Healthy Skepticism of Authority

# Thanks

Help make it happen!

<https://reproducible-builds.org/contribute/>

<https://reproducible-builds.org/donate/>

<https://reproducible-builds.org/who/sponsors>



# Copyright and attributions

Copyright 2016-2025 Vagrant Cascadian <[vagrant@reproducible-builds.org](mailto:vagrant@reproducible-builds.org)> Portions by contributors to the reproducible-builds.org website.

This work is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License.

To view a copy of this license, visit <https://creativecommons.org/licenses/by-sa/4.0/>

Cover art derived from [https://en.wikipedia.org/wiki/File:Never\\_Mind\\_the\\_Bollocks,\\_Here%27s\\_the\\_Sex\\_Pistols.png](https://en.wikipedia.org/wiki/File:Never_Mind_the_Bollocks,_Here%27s_the_Sex_Pistols.png) and modified by Vagrant Cascadian.

960px-Supply\_and\_demand\_network\_english.svg.png Downloaded from:

[https://commons.wikimedia.org/wiki/File:Supply\\_and\\_demand\\_network\\_\(en\).svg](https://commons.wikimedia.org/wiki/File:Supply_and_demand_network_(en).svg)

Copyright Andreas Wieland, licensed under GFDL without invariants or various CC-BY-SA versions.