Never Mind the Checkboxes, Here's Reproducible Builds!

Vagrant Cascadian & Chris Lamb

FOSSY 2025-08-02

Cover Art

Who we are

A small part of the Reproducible Builds Community

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

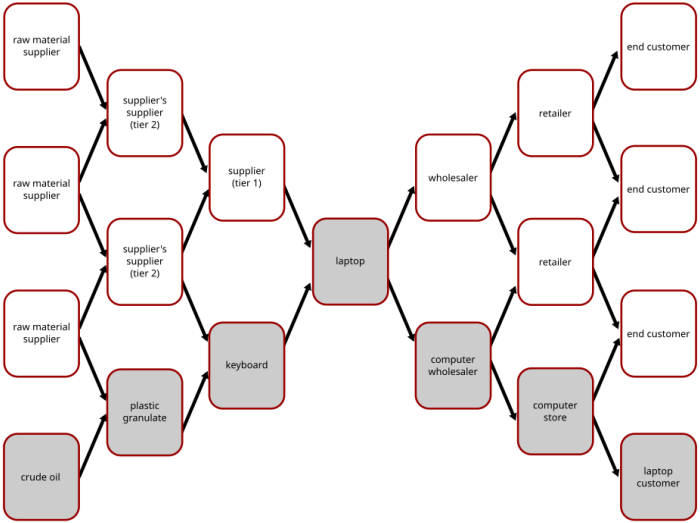
- ...
- Autonomy
- Independence
- Mutual Aid
- Community
- DIY

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`

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

Software is nearly infinitely and instantaneously duplicated and transmitted

Hardware gets moved around slowly, requires many steps to duplicate

Billy O Material

`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.

Software Bill Of imMaterials

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.

ISO9000

https://en.wikipedia.org/wiki/ISO_9000_family
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

ISO9000

https://en.wikipedia.org/wiki/ISO_9000_family
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

ISO9000

`https://en.wikipedia.org/wiki/ISO_9000_family`
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

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

- 2024

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

- 2024
- Europe

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

- 2024
- Europe
- Voluntary self assessment

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

- 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

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
- United States of America

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
- United States of America
- SolarWinds and other big incidents

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- Not yet rescinded

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- Not yet rescinded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

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- Not yet rescinded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

OpenChain

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

- ...

OpenChain

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

- ...
- Voluntary self assessment

OpenChain

`https://openchainproject.org/checklist-iso-dis-18974`

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

OpenChain

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

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

OpenChain

`https://openchainproject.org/checklist-iso-dis-18974`

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

OpenChain

`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

OpenChain

`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

OpenChain

`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)

OpenChain

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

OpenChain

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

OpenChain

`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

OpenChain

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

OpenChain: The Security Stuff

`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

Real problems

do they solve actual problems?

Quality

Does it improve the quality of software?

SBOM

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

- ...

SBOM

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

- ...
- list of software dependencies

SBOM

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

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

SBOM

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

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

Goals

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

Signatures

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.

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

Reproducible builds of Free and Open Source Software

- ...

Reproducible Builds

Reproducible builds of Free and Open Source Software

- ...
- Autonomy and Independence

Reproducible Builds

Reproducible builds of Free and Open Source Software

- ...
- Autonomy and Independence
- Mutual Aid

Reproducible Builds

Reproducible builds of Free and Open Source Software

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

Reproducible Builds

Reproducible builds of Free and Open Source Software

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

Reproducible Builds

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