Security Concerns in Proprietary and Opensource Software

Julian Drexler

Agenda

- Introduction
- Security Overview
- Open-Source Software
- Proprietary Software
- Comparison

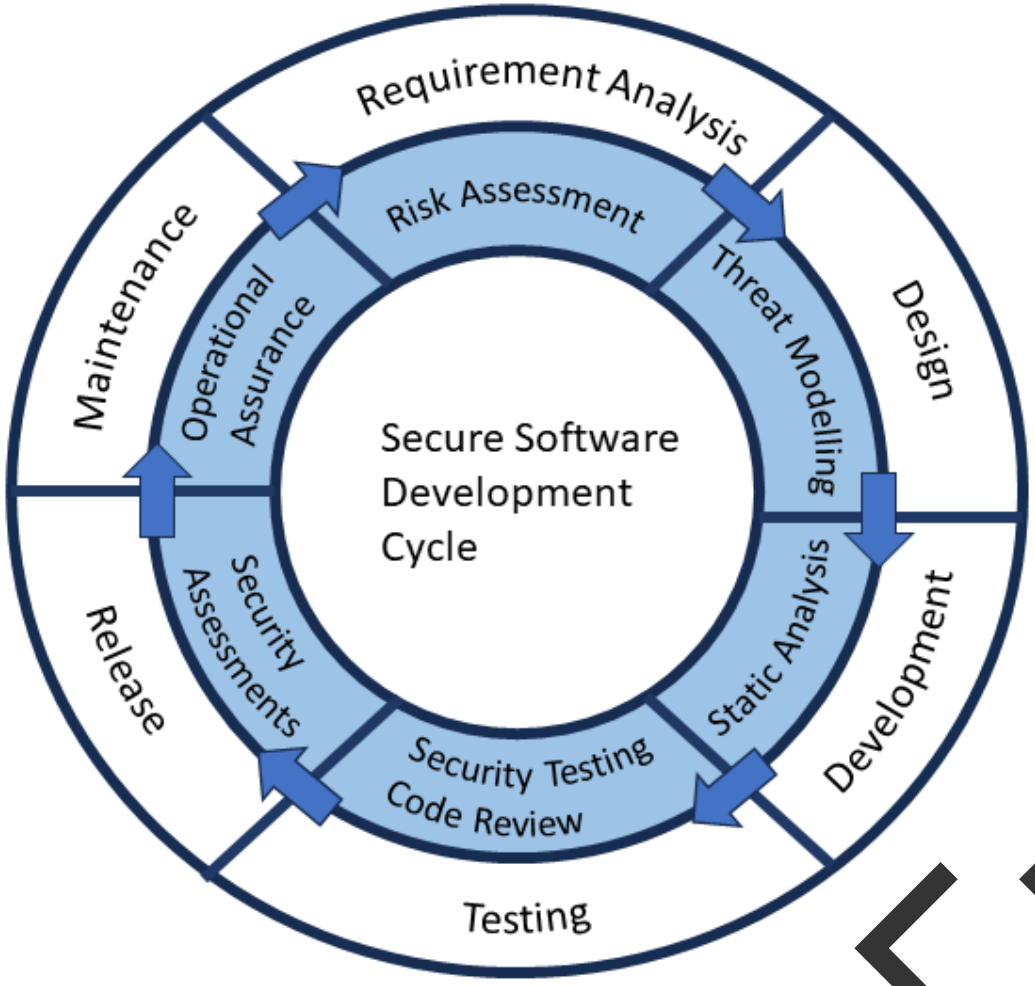
Introduction

- 2022 around 25.082 vulnerabilities were made public [1]
- Enterprise open source gaining market share [2]

Security Overview: Goals

- Authenticity
- Integrity
- Confidentiality
- Availability
- Non-Repudiation
- Anonymisation

Security Overview: Development - Process



(own representation)

Security Overview: Development - Methods

- Static Code Analyse (SAST)
- Dynamic Application Testing (DAST)
- Software Composition Analysis (SCA)

Open Source: Definitions

- Open Source Initiative
- Free Software Foundation

Open Source: History

4 Phases [3] + 1

1. Collective inventions - 1950’s
2. Commodification and Emerging Subcultures - 1960’s
3. Institutionalization – 1980’s
4. Growth – 1998
5. (Large Acquisitions – 2015)

Open Source: Licencing

- Strong Copyleft Licence
  - GPLv3.0
- Weak Copyleft Licence
  - LGPL 2.1
- Non Copyleft Licence
  - Apache 2.0

Open Source: **Maintenance** and Organization

- Maintenance
  - Contributions: top 3 motivations are non-monetary [4]
  - Open-source projects can get abandoned

Open Source: Maintenance and **Organization**

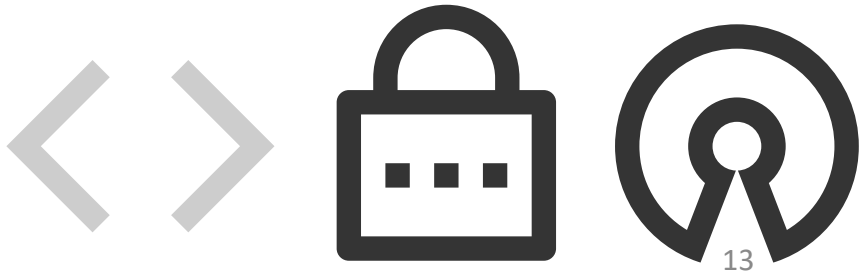
- 3 Phases [5]
  - Non formal coordination
  - Internal governance
  - Governance towards outside parties
- Approaches [6]
  - Autonomous
  - Associated
  - Integrated

Open Source: Funding

- Foundations and project communities
  - Donations
  - Code contributions
- Open-source companies
  - code contributions
  - 7 open-source business model archetypes [7]

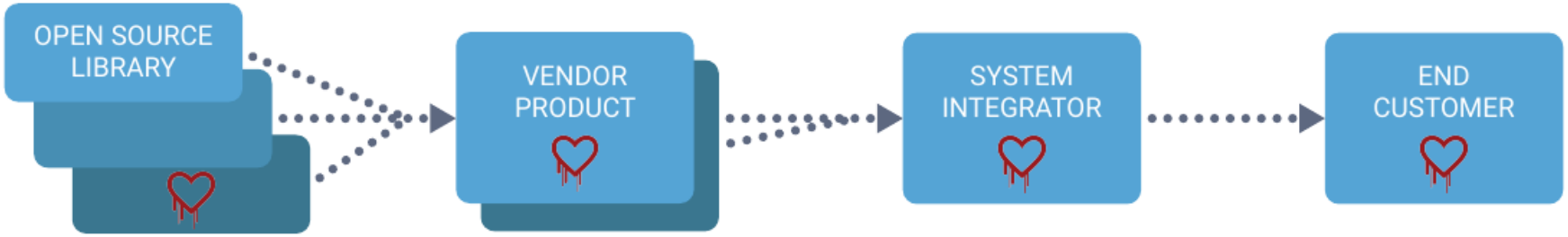
Open Source: Security

- Improvements through processes, tools and knowledge
- Survey: 89% think that open source is more secure than proprietary [2]
- Auditable by everyone



Open Source: Security Issues Examples

- 9.658 new vulnerabilities in 2020 (50% increase to 2019) [8]
- OpenSSL: Heartbleed (2014)
- Log4j: Log4Shell (2021)



Source: Synopsys, Inc. (2017) *Diary of a Heartbleed*. Available at: https://www.synopsys.com/content/dam/synopsys/sig-assets/whitepapers/diary-of-heartbleed.pdf.

Proprietary Software: Definition and Licencing

- 45% of enterprise software is proprietary [2]
- Ownership
- Licences for proprietary software

Proprietary Software: Maintenance

- 25% - 33% development efforts of creating the software [9]
- Outdated software in supply chains

Proprietary Software: Open-Source Components

- 96% have open-source components [10]
- Licence conflicts
- Maintenance
- Contributions to open-source

Proprietary Software: Security

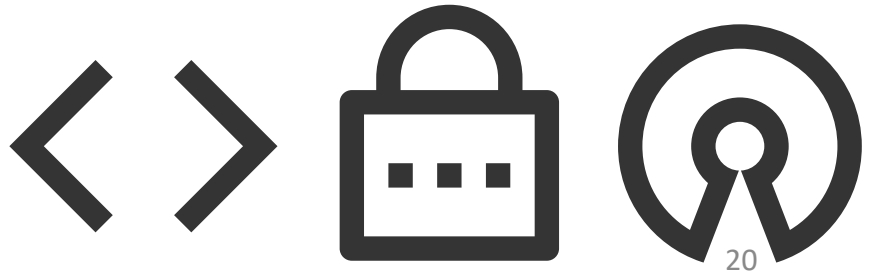
- “Black box”
- Vulnerabilities can hide
- Reverse Engineering
- Supply chain attacks

Proprietary Software: Security Issues Examples

- Windows SMB Protocol: EternalBlue (2017)
- CCLeaner: Supply chain attack (2017)

Comparison

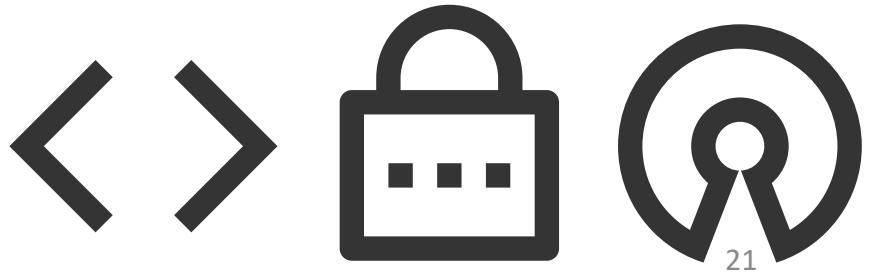
- Transparency and trust
- Security issues reporting



Conclusion and Discussion

- Many factors are influential

- Bias information on surveys and on security reports
- General view on Software



Questions?

References

[1] SecurityScorecard (2023) Security Vulnerabilities Published In 2022. Available at: https://www.cvedetails.com/vulnerability-list/year-2022/vulnerabilities.html

[2] Gordon Haff (no date) The State of Enterprise Open Source 2022. Red Hat Inc. Available at: https://www.redhat.com/en/enterprise-open-source-report/2022.

[3] Schrape, J.-F. (2016) Open-Source-Projekte als Utopie, Methode und Innovationsstrategie: historische Entwicklung - sozioökonomische Kontexte - Typologie. Glückstadt: vwh, Verlag Werner Hülsbusch, Fachverlag für Medientechnik und -wirtschaft (Medienwirtschaft).

[4] Frank Nagle et al. (2020) Report on the 2020 FOSS Contributor Survey, The Linux Foundation & The Laboratory for Innovation Science at Harvard. Available at: https://www.linuxfoundation.org/resources/publications/foss-contributor-2020.

[5] De Laat, P.B. (2007) 'Governance of open source software: state of the art', Journal of Management & Governance, 11(2), pp. 165–177. Available at: https://doi.org/10.1007/s10997-007-9022-9.

[6] Eckert, R., Stuermer, M. and Myrach, T. (2019) 'Alone or Together? Inter-organizational affiliations of open source communities', Journal of Systems and Software, 149, pp. 250–262. Available at: https://doi.org/10.1016/j.jss.2018.12.007.

[7] Duparc, E. et al. (2022) 'Archetypes of open-source business models', Electronic Markets, 32(2), pp. 727–745. Available at: https://doi.org/10.1007/s12525-022-00557-9.

[8] Adam Murray (2021) All About Mend's 2021 Open Source Security Vulnerabilities Report. Available at: https://www.mend.io/blog/2021-state-of-open-source-security-vulnerabilities-cheat-sheet/ (Accessed: 19 November 2023).

[9] Zelkowitz, M.V. (1978) 'Perspectives in Software Engineering', ACM Computing Surveys, 10(2), pp. 197–216. Available at: https://doi.org/10.1145/356725.356731.

[10] SYNOPSIS Inc. (2023) 2023 OPEN SOURCE SECURITY AND RISK ANALYSIS REPORT. 8. Available at: https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html.