Context and Motivation

• Defense of the Software Supply Chain is a key component of the May 2021 Executive Order 14028 to Improve Nation’s Cyber Security
The Office of the National Cyber Director (ONCD) Initiative

• Identified three lines of effort (LOE):

  • LOE 1: Enhance and Invest in Secure and Transparent OSS Development

  • LOE 2: Improve Transparency of Supply Chain Data through SBOM

  • LOE 3: Collaborate with Cyber Defenders to Understand and Mitigate Software Supply Chain Risk
The Office of the National Cyber Director (ONCD) Initiative

• Identified three lines of effort:

  • LOE 1: Enhance and Invest in Secure and Transparent OSS Development
  • LOE 2: Improve Transparency of Supply Chain Data through SBOM
  • LOE 3: Collaborate with Cyber Defenders to Understand and Mitigate Software Supply Chain Risk
Expert Engagement

• Goals:

• generate ideas and broad discussion around key approaches to invest in the security of open-source software
Expert Engagement

• Timeline:

  • April/May 2022: Steering Committee (SC) is formed and uncovers themes and challenges for further discussion

  • August 2022: two-day workshop for ~30 stakeholders informed by SC meeting take-aways

  • September 2022: public report guiding outcomes of LOE 1 and USG future investments
Main Themes

• Memory-Safe Programming Languages

• Dependency Management

• Behavioral and Economic Incentives to Secure the Open Source Software Ecosystem
Behavioral and Economic Incentives to Secure the Open Source Software Ecosystem
The Issue

- Software is produced by humans and consumed by humans

**Used by 161k**

**Contributors 3,014**

+ 3,003 contributors

**Languages**

- C++ 61.9%
- MLIR 4.0%
- Starlark 3.0%
- HTML 2.6%
- Go 1.1%
- Other 2.5%
Socio-technical issues

Used by 161k

Contributors 3,014

Languages

- C++ 61.9%
- Python 24.9%
- MLIR 4.0%
- Starlark 3.0%
- HTML 2.6%
- Go 1.1%
- Other 2.5%
OSS Ecosystem: Who are the Participants?

Producers

Consumers

Software developers

Organizations

Producers
Software Developers

• Humans who contribute (e.g., code, management) with the OSS ecosystem:
  • non-paid volunteers
  • compensated professionals

• Busy, overwhelmed

• Primary tasks is not necessarily security

• Lack incentives to operate with a security mindset:
  • Is it even possible given the high cognitive demands of producing functionality?
Organizations

• Companies that produce OSS

• Not liable for vulnerabilities in the code they produce
Consumers
Software Developers

• Humans who use OSS via dependencies in their own code
Organizations

• Have products and services that depend upon OSS code
Consumers Lack...

- **Trust** in the code they consume
Consumers Lack...

• **Transparency** on their dependencies

Consumers Lack...

- **Guidance** and **awareness** on how to consume third-party code in a trustworthy manner
Consumers Lack...

- **Situational awareness** for when trust is violated

Source: https://commons.wikimedia.org/wiki/File:Tamper_evident_seal_on_OTC_pharmaceutical.jpg
Key Question

How to create and maintain behavioral and economic incentives for these diverse stakeholders to operate in a way that foster a more secure OSS ecosystem?
Challenges

• Diversity of stakeholders and roles:
  • Producers vs. Consumers
  • Developers:
    • Paid vs. unpaid
    • project/team size
    • security expertise
  • Organizations:
    • small vs. large
    • sector: industry vs. government
Challenges

• Incentives not aligned or at odds with one another:
  
  • Producers:
    • Time-to-Market
    • “security is the consumer’s responsibility”

  • Consumers:
    • “I want trustworthy code that does not break existing code”
Main Take-Away for Theme

Unknowns >> Knowns
Potential Reason for Unknows

Socio-technical security issues of the OSS ecosystem

Source: https://www.alimed.com/optivisors-and-optivisor-magnifier-lens-plates.html?pid=58400&gclid=Cj0KCQjwvZCBhCiARIsAPXbajt67fbRpbDMvO68P9X5DW3nwhV8yyARtAViOJk_KctU0i3oT6ZCq5UaAgDfEALw_wcB
Socio-Technical Security Issues of OSS Ecosystems

• Multidisciplinary problem

Computing/Cyber Security + Social, Behavioral and Economics

• We need to catalyze multidisciplinary research on these issues
Economics
Research Questions

1. What are the incentives driving each stakeholder?

   - How can we leverage and/or align these incentives among this diverse group to create a more secure OSS ecosystem?
Research Questions

2. How to characterize/measure:

• Project exposure to security risks

• Trust (in developers, dependencies, projects)

• Return of Investment (ROI) of implementing secure software development practices

• Economic harm of keeping the status quo
Research Questions

3. To what extent accountability/liability helps in fostering security practices in software development?

• How to operationalize and implement accountability/liability?
• Is it even possible and/or desirable?

Research Questions

4. How to support the wide variety of project sizes, especially the very small contributor team on a very important project?
Software Development Practices
Research Questions

1. Why people decide to adopt or not a secure approach?
   • How to measure this quantitatively?

2. To what extent security audits help in preventing security risks and vulnerabilities?
Research Questions

3. In which conditions does monetary compensation translates into more secure software development practices?

4. How to include security training that is appropriate for everyone?
   • seniority level
   • security experience
   • project size/type
   • organization size/type
Research Questions

5. To what extent hiring security specialists for OSS projects translates into more secure software being developed?

6. What type of usable security tooling is needed to streamline secure software development practices?
Team Dynamics
Research Questions

1. How to detect social engineering attacks in OSS projects?
   • How to identify attackers?
   • How to identify tactics of persuasion?
Research Questions

2. How to detect suspicious developer ascendency in projects?
   • How are people embedded into OSS projects?

3. Is toxicity in team communications associated with less secure software development practices?

Source: https://freesvg.org/censored-swear-word-vector-image
Evaluation
Research Questions

1. What are the criteria to evaluate success in adopting socio-technical measures for a more secure OSS ecosystem?
Technical Recommendations
Concurrent with More Research...

1. Pay maintainers:

• There should be requirements to pay into organizations that support community and/or security practices if one gets a government contract for projects that use OSS.
Concurrent with More Research...

2. Tooling to support dependency transparency:

• SBOM metadata:
  • including presence of code in unsafe languages

• To what extent project is depended on OSS

• Security/vulnerability score of OSS components that make up project

• Reporting of suspicious packages
Concurrent with More Research...

3. Metrics:

- Quantification of risk and dependency
- Mean time to remediation
- Criteria for a project to be defined as critical
Thank you!

doliveir@nsf.gov