



Securing Open Source Software

Dr. Nicko van Someren, CTO, The Linux Foundation
NCSC One Conference, May 16th, 2017

Open Source is huge and it's here to stay

3.8M

Open Source
Contributors
World Wide

31B

Lines
committed to
open source
repositories

110+

Open
technology
startups that
raised funding

10

Open
technology
companies
valued above
\$1B

\$2.4B

Venture
dollars invest
in open
companies
2014

Source: Accel Ventures



**Open Source projects are the
roads and bridges of the internet**



Roads and bridges need to be maintained

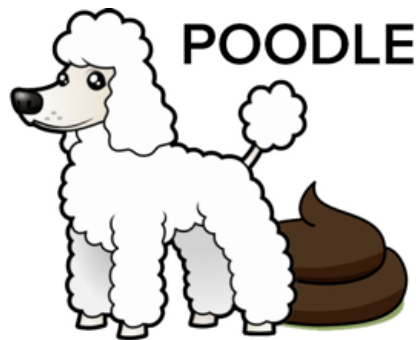
Sometimes open source breaks...




```
bash
$ env x='() { :; }; echo vulnerable'
```



Shellshock



A portrait of Linus Torvalds, a man with short brown hair and glasses, wearing a black t-shirt and a small yellow microphone. He is looking slightly to the right. The background is a plain, light-colored wall with a large, faint, stylized '@' symbol on the right side.

Linus's Law: "Given enough eyeballs, all bugs are shallow."

What if you don't have enough eyeballs?

FOSS is not more or less secure, but it is different

- Typically there is a more diverse set of people contributing
 - Often serially, over a long period of time
- Sometimes (often?) there is a culture of “code is more important than specification”
- Processes are often more ad hoc
- Code often starts as a research project or PoC, then gets released and takes on a life of its own

Many critical projects have been under-resourced

- OpenSSL
 - Run by millions of businesses
 - Got < \$3,000 in support in 2013
- NTPD
 - Run by every major stock exchange
 - Some code is 35 years old
 - Maintained by one guy, part time
- Bash
 - Maintained by one guy
- GnuPG
 - One maintainer, going broke
- OpenSSH
 - Maintainer works odd jobs...
- You get the picture...



The Core Infrastructure Initiative

The Core Infrastructure Initiative

- The CII aims to substantially improve security outcomes in the OSS projects that underpin the Internet
- The CII funds work in security engineering, security architecture, tooling, testing and training on key OSS projects, as well as supporting general development on security-specific projects (such as crypto libraries)



Bloomberg



facebook

FUJITSU

Google

HITACHI
Inspire the Next



NEC



vmware™

CII is a non-profit, funded by membership donations, largely from the tech industry

What can we do to improve the security of Open Source Software?

We can do all the same things as we do when building commercial software

The big difference is that we have to do it collaboratively, without having a top-down mandate demanding it

Security is a process, not a product

- Think about security early. Think about security often.
- This requires buy-in from the whole project community

Fostering a culture of security within your open source project is the single most important thing that you can do to improve your security outcomes
- Security needs to be given equal weight with scalability, performance, usability and all the other design factors that matter to your users

So what is CII doing?

Multiple pillars to the CII's approach

- Find where the risky projects are
- Help them fix their own code
- Support the development of better OSS security tools
- Teach developers to use security tools
- Convince developers that security is a priority

Finding out where the risks are

- Which projects are important to users?
 - What are the historic trends for bug and vulnerability density?
 - How responsive are the developers?
 - What is the health of the developer community?
-
- Results published through the CII Census project

Tactically fix critical projects that are broken

- Maintenance work is not fun, but it's vital
- Pay developers to work on key projects full time
 - Projects must decide what needs to be done in an open process
- Match willing and able developers to relevant projects
 - Security experts are needed by all sort of projects
- Encourage educational establishments to get students involved
 - Fixing broken old code is great practice for real life!

Improving open source security tooling

- Fund development of new or improved OSS security tools
- Support the creation of frameworks for automated and continuous security testing
- Develop ways to make security test tools easier to use
- Write (or pay for writing of) guides and documentation for how to deploy continuous security testing
- Work with OSS hosts to make tools easier to integrate

Drive better security *process* in OSS projects

- CII Badge program is an open process for evaluating **security processes** in OSS
- Free program designed with evolving criteria from open source community
- Receiving a badge allows a project to showcase its commitment to security
- Both the web tool and the criteria are developed as open source projects
- No security theatre - only include items that really improve security



Evangelism and Building community

- Hosting or co-sponsoring events on OSS security and resilience
- Supporting travel for developers to present at conferences
- Fund travel to allow key OSS developer teams to meet face to face in order to set priorities and plan future work

Conclusions

- The internet, and every business built on it, depends on Open Source Software
- Open Source Software is developed communally and we have a communal responsibility to keep it secure, for the sake of everyone
- Key to securing these foundation stones of the internet is making sure that secure development practices are prioritised by the teams of developers who build these shared assets
- Fixing old code isn't fun, and it isn't sexy, but it's critical, and we often have to pay someone to do it!



Thank you!

<https://www.coreinfrastructure.org>

nicko@linuxfoundation.org