Table of Contents

A Message from the Executive Director ....................................................... 4

World’s Largest Industry Giants Securing Open Source Software ....................................................... 8

A Message from the Programme Director ..................................................... 10

CII Invests In More Than 14 Projects - 2016 Milestones and Successes ..................................................... 12

Bringing the Open Source Security Community Together ..................................................... 20
A Message from Nicko van Someren, Executive Director

The CII’s mission is to ensure that the open source code that underpins business today is secure and resilient. By providing tools, expertise and direct funding, we are helping to fortify the open source software on which the modern world relies. We’ve made great strides this year, and we are proud of these achievements, but we also recognize that the Internet is comprised of thousands of open source projects, many of which are in need of more work, more resources and more protection.

Despite dependency by a huge number of enterprises, the open source core Internet infrastructure remains undervalued and under-resourced. Yet, without the CII’s funding, services and programs, many open source projects would be more vulnerable and less resilient than they are today. Worse yet, some might not even exist.

We’ve made real progress and achieved many of our initial objectives, including our goal to make OpenSSL significantly more secure, fixing many of its bugs and reducing the chance of introducing new bugs. OpenSSL is no longer in fire-fighting mode. In the absence of crisis and uncertainty, the project has been able to drive proactive security reviews and processes. We can now say with confidence that this critical infrastructure is much less likely to have a major vulnerability in the future.

While the CII remains closely associated with OpenSSL, which we continue to support, we’re now at the point where we also proactively identify and seek out new projects to support. Input from our advisors, steering committee and the CII-sponsored Open Source Census Project, which analyzes popular open source projects, helps us identify the ones at risk and in need of further testing and assistance. To support this expansion of efforts, in 2016 we rolled out a new online grant submission process, which has made reviews and voting much swifter and more fluid, allowing developers to be funded at a much faster rate.

Our initial mandate was to secure the projects that are most critical to businesses on the Internet. In order to make the biggest impact possible, the CII targets the broadest range of projects possible within this remit: established and new, large and small, infrastructure and front-facing. Yet, it’s not always easy to predict which Internet technologies will take off. Just a few years ago, hardly anyone would have predicted that one of the fastest-growing server-side projects around would involve JavaScript with Node.js (instead of .Net or C#). Furthermore, not all open source projects have a security-first mindset. Using a combination of expert input and community feedback (and some educated guesswork), the CII is working not just to protect the projects that underpin business now, but also to ensure that the core infrastructure of tomorrow is secure before it ever goes into service.

In 2016, we have also transitioned from providing more tactical aid to delivering longer-term and more strategic support. For example, our work on the aforementioned Open Source Census project is evolving to include more sophisticated data analysis and operate on a continuous basis rather than simply deliver a snapshot. We also hope to leverage this project for industry education. Other CII programs are designed to inspire a set of behaviors that will spontaneously instill software security best practices universally. For example, the CII Best Practices Badges effort helps encourage practices known to improve software security outcomes while supporting projects such as Frama-C, which provides re-usable tools to catch bugs before they reach the field.

“Our initial mandate was to target the projects that are most critical to businesses on the Internet. In order to make the biggest impact possible, the CII targets the broadest range of projects possible within this remit: established and new, large and small, infrastructure and front-facing.”
The CII Best Practices Badges deserves to be called out as a particular success. Since formally launching in May 2016, more than 400 projects have signed up for the process and more than 50 projects have earned the badge. We specifically reached out to both smaller projects, like cURL, and bigger projects, like the Linux kernel, to ensure that our criteria made sense for many different kinds of projects. The list of projects that proudly display the badge continues to grow and currently includes GitLab, Node.js, OpenBlox, OpenSSL, OpenStack, OPNFV, and Zephyr.

Although the CII has helped make the Internet safer, our job is not yet done and, in all likelihood, will never be done. Until we achieve a wholesale mindset change in how we engineer software, the need for CII will not diminish. In the meantime, the CII will continue to tackle open source security on multiple fronts: providing the tools, training and testing infrastructure that projects need as well as the tactical support needed to fix existing legacy code.

As we look ahead to 2017, we need to continue to raise awareness of the importance of open source software, and we need to get more businesses, as well as governmental and non-governmental organisations, involved in furthering our efforts. With massive chunks of the Internet continuing to move away from proprietary software, we’re more dependent than ever before on open source. CII’s work is never-ending and ever-expanding as more open source becomes core infrastructure. Given the enormity of the challenge, we readily admit that there is much more CII needs to accomplish.

We are excited by the challenge of improving the security of core Internet infrastructure and spreading secure coding best practices even further. We extend our sincere gratitude to our members and advisors who continue to work closely with us to fortify our critical infrastructure. We look forward to continuing this work in 2017.

Nicko van Someren, Executive Director

Sue Graves, director of client experience at the Network Time Foundation, and Leah, a NTF volunteer, attended the Combined Federal Campaign Charity event to help raise additional funds and awareness for the Network Time Foundation.
World’s Largest
Industry Giants Securing
Open Source Software

The Core Infrastructure Initiative is deeply grateful to our 19 founding members for their continuing support. Without their investment we would not be able to carry out this important work.
A Message from Marcus Streets, Programme Director

My key role as the Programme Director for CII is to manage the spend side of the budget and work directly with the developers we assist. Without the type of aid CII provides, projects falter. Unless there is a critical mass of developers able to devote time, projects are at risk of a vulnerability like Heartbleed.

We currently support more than 20 developers on 14 projects. They are based across Australia, Canada, Europe and the United States. However, even with a narrow definition, this is only a small fraction of the projects that fit the description of core infrastructure. We must carefully target funding to widely used projects that do not currently have the resources to support a full-time developer base.

One challenge we’ve encountered this year is finding skilled people to take on the work. While the desire to work on open source exists, without compensation it’s simply not feasible for many developers to do so. Emese Renfy, for example, had to step back from Kernel Self Protection Work because funding from CII took so long to approve. We’ve worked to resolve this with our new online grant system. Another solution is to find those who are already working on open source as a hobby and allow them to continue their work at a fully-funded, professional level. For example, Chris Lamb and Ximin Luo, have been able to give up their day job to focus exclusively on the Reproducible Builds project.

CII has also been instrumental in bringing the communities working on securing open source software together. From LinuxCon Berlin this past fall, to the upcoming 2nd Reproducible Builds World Summit, CII makes it possible for developers we fund to work more closely together to advance their design and development work. This support ranges from providing meeting venues to sponsoring travel and accommodation for attendees who would not otherwise be able to afford attending events around the world.

I’m inspired to work with such adept and dedicated developers. With a healthy pipeline of grants to review in the new year, I’m confident we’ll be able to expand CII’s reach and grow the pool of talent working on core infrastructure even further.

Marcus Streets, Programme Director
CII Invests In More Than 14 Projects - 2016 Milestones and Successes

With backing from CII, the Reproducible Builds team recently met in Berlin at the 2nd Reproducible Builds World Summit.

How the CII Spends its Funds

- Strategic
  - $192K
  - Frama-C
- Best Practice Badge
  - $120K
- Long-term
  - Census
  - $120K
- Reproducible Builds
  - $250K
  - Reproducible Project
- Short-term
  - $150K
  - NTPSec
- Kernel Self Protection
  - $60K
- Tactical
  - OpenSSH
  - $50K
- Bouncy Castle
  - $50K
- OpenSSL
  - $50K
- OpenSSL Audit
  - $20K
- Fuzzing Project
  - $10K
- ntpd
  - $160K

- Developer library
- Educational effort
- Testing tool or project
- System tool or application
- Developer tool
**THE LEGION OF THE BOUNCY CASTLE**

The Bouncy Castle Crypto package is a Java implementation of cryptographic algorithms developed by the Legion of the Bouncy Castle, an Australian charity.

With help from CII, this organization recently completed work on the Java Secure Socket Extension (JSSE), which provides access to Secure Socket Layer (SSL) and Transport Layer Security (TLS) implementations.

“With CII helping to sponsor our work, we’ve made the project more stable, which led to Google and Intel’s security teams providing testing and analysis of the APIs in ways we could not have previously imagined. Collaboration and work like this, which will improve the overall quality and security of the APIs, would be difficult, if not impossible, to take advantage of effectively if we were not able to devote sufficient time to them.”

- David Hook, Founder, Bouncy Castle Cryptography Project

**OPENSSL**

OpenSSL is the most widely used Open Source general-purpose cryptography library. It provides a robust, commercial-grade, and full-featured toolkit for the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols.

CII continues to fund core developers Steven Henson and Andrey Polyakov, who have improved security governance by introducing formal code review requirements, policies for change control and bug handling.

With more collaborative architecture reviews now in place, bugs are found and closed faster, security updates are deployed more quickly and security roadmap items are advanced more quickly.

**OPENSSL AUDIT**

CII commissioned the global cyber security and risk mitigation firm NCC Group to perform a full audit of OpenSSL.

The audit’s primary focus is on the TLS stacks, covering protocol flow, state transitions, and memory management.

**TIS-INTERPRETER (FRAMA-C)**

Frama-C is an extensible framework for source code analysis. CII sponsored the work of Pascal Cuq, who released the open source version known as TIS Interpreter.

This included all the extensions necessary to support the false-positive-free operation on OpenSSL, which has led to dozens of bugs being closed.

“Support from CII is enabling us to work on detecting strict aliasing violations, a class of issues common in legacy C code that no current sanitizer is able to help with.”

- Pascal Cuq, Co-Initiator of the Frama-C Project

**BEST PRACTICES BADGES PROGRAM**

This free program helps determine security, quality and stability of open source software. Since formally launching in May 2016, more than 400 projects have signed up for the process and more than 50 projects have earned the badge, including GnuPG, LibreOffice, Node.js, OpenSSL, OpenStack and OPFNV. The app and its criteria are an open source project that developers can contribute to.

“Support from CII is enabling us to work on detecting strict aliasing violations, a class of issues common in legacy C code that no current sanitizer is able to help with.”

- Pascal Cuq, Co-Initiator of the Frama-C Project

**Educational Effort**

“Support from CII is enabling us to work on detecting strict aliasing violations, a class of issues common in legacy C code that no current sanitizer is able to help with.”

- Pascal Cuq, Co-Initiator of the Frama-C Project

“I can definitely confirm that the CII Badging Program has helped us improve ZAP quality. It allowed us to see where we were doing well and where we were falling short. This helped us focus on the areas that needed the most improvement. For us, it has definitely not been a ‘box ticking’ exercise.”

- Simon Bennetts (a.k.a. psiinon), OWASP ZAP Project Lead
System Tool or Applications

GNUPG

GnuPG is a complete and free implementation of the OpenPGP standard. GnuPG allows developers to encrypt and sign data and communication, features a versatile key management system as well as access modules for all kinds of public key directories.

CII's continued support in 2016 advanced development on many fronts, including setup of a Jenkins server, use of Clang tools for static code analysis and introduction of a new regression test suite for non-native builds (Windows). The project has also been able to fix several real bugs and numerous other warnings as well as deliver many new features. The first OpenPGP conference was also possible thanks to CII assistance.

"The CII grant was a solid base for me to manage the development and to work on acquiring other financial sources. Thank you for supporting GnuPG in this way." - Werner Koch, GnuPG Founder

KERNEL SELF PROTECTION

KSPP is an operating system hardening project with the goal of eliminating classes of vulnerabilities in the Linux kernel.

CII supported Emese Renfy for six months from January to July working on the constify, latent_entropy, structleak and initify plug-ins.

As of November, CII is currently supporting David Windsor, who is working on the Hardened.Atomic and Hardened.Usercopy plug-ins.

NTPSEC

NTPsec project is a secure, hardened implementation of Network Time Protocol derived from Network Time Protocol (NTP) Classic, Dave Mills’s original.

CII supported the project lead who was able to refactor old code and reduce the code base by two-thirds without losing functionality. This means NTPSec has avoided many of the recent security issues with classic NTP.

"Over the last nine months alone, Harlan has worked diligently on NTP development, bug fixes, security hardening and enhancements." - Sue Graves, Director of Client Experience, Network Time Foundation

NTPD

The Network Time Protocol Daemon (ntpd) is an operating system program that maintains the system time in synchronization with time servers using the NTP.

The CII's funding has had a significant positive impact on NTP's development and improvement.

To harden the code even further, Harlan Stenn has worked with the Network Time Security (NTS) design team on a proof-of-concept release. Once NTS is completed, it will be rolled into the NTP Project's Reference Implementation.

OPENSSH

OpenSSH is the most widely used secure remote access shell tool. It provides secure authentication and encrypts all traffic to effectively eliminate eavesdropping, connection hijacking and other attacks.

This open source implementation of the IETF SSH protocol is the dominant choice in open source operating systems, and also in commercial products like high-end routers and switches.

Along with others from his team, Theo de Raadt has been able to continue his work on the open source implementation of the SSH protocol, releasing OpenSSH 7.3p1 in August because of CII aid.

CII support makes it possible for developers to come together to advance development of projects.
Testing Tool or Project

REPRODUCIBLE BUILDS PROJECT

Reproducible builds are a set of software development practices that create a verifiable path from human readable source code to the binary code used by computers.

CII funded Holger Levsen and Jérémy Bobbio’s efforts to eliminate unneeded variations from the build processes of thousands of free software projects. Their efforts, combined with those from the rest of the Reproducible Builds Project, have resulted in 91 percent of the packages within the Debian testing distribution becoming reproducible. More recently, CII extended the grant to include Debian developers Chris Lamb, Mattia Rizzolo, Ximin Luo and Vagrant Cascadian, as well as Ed Maste, working with FreeBSD.

“Our work has already made significant progress in Debian GNU/Linux, and we are making our tools available for Fedora, Guix, Ubuntu, OpenWrt and other distributions. Support from CII allows us to work on the infrastructure required to make Reproducible Builds both meaningful and approachable for end-users.” - CHRI LAMB, DEBIAN DEVELOPER

FUZZING PROJECT

Security researcher Hanno Böck spearheads The Fuzzing Project, coordinating fuzzing efforts for open source software. The fuzzing software testing technique is an easy and powerful way to identify security problems in software.

With funding from CII, Hanno Böck created a Linux system that was fully tested with Address Sanitizer.

“The Fuzzing Project contributed a large number of bug reports and fixes to a variety of open source projects. Most notable is an effort to mass-test software with the compiler feature Address Sanitizer, which uncovered countless bugs, ranging from low-level system tools like syslog-ng or bash to desktop environments like GNOME and KDE.” - HANNO BOCK, PROJECT MANAGER

CII backs David Wheeler’s ongoing work on the Census, which is evolving to include both sophisticated data analysis and continuous updates.

OPEN SOURCE CENSUS

By funding the work of David Wheeler, CII launched and now maintains the Open Source Census Project, which analyzes popular open source projects to help identify the ones at risk and in need of further testing and support.

OWASP ZED ATTACK PROXY (ZAP)

The OWASP Zed Attack Proxy (ZAP) is one of the world’s most popular free security tools and is actively maintained by hundreds of international volunteers. CII supported bringing on a full-time developer, who is working on adding multi-user, multi-role functionality and improving the user interface, as well as general maintenance.

“The CII grant has had an immediate impact on OWASP ZAP. We’ve added a developer, improved coding best practices, set up a predictable release schedule and roadmap, and performed audits to help future-proof our code.” - SIMON BENNETTS (A.K.A. PSIINON), OWASP ZAP PROJECT LEAD

Aid from CII allows Pascal Cuoq, co-initiator of the Frama-C project, to continue developing and promoting Frama-C—as well as energizing the user community.

“The CII grant has had an immediate impact on OWASP ZAP. We’ve added a developer, improved coding best practices, set up a predictable release schedule and roadmap, and performed audits to help future-proof our code.” - SIMON BENNETTS (A.K.A. PSIINON), OWASP ZAP PROJECT LEAD
Bringing the Open Source Security Community Together

- **4** conferences
- **MORE THAN 100** people attended
- **$75k** in travel grants
- **MORE THAN 60** travel grants awarded to developers
- **NEARLY 24k** articles globally, increase of 36% over 2015

WWW.COREINFRASTRUCTURE.ORG