LINUX FOUNDATION

CORE INFRASTRUCTURE INITIATIVE

Core Infrastructure Initiative Discussion

Emily Ratliff

August 20, 2015

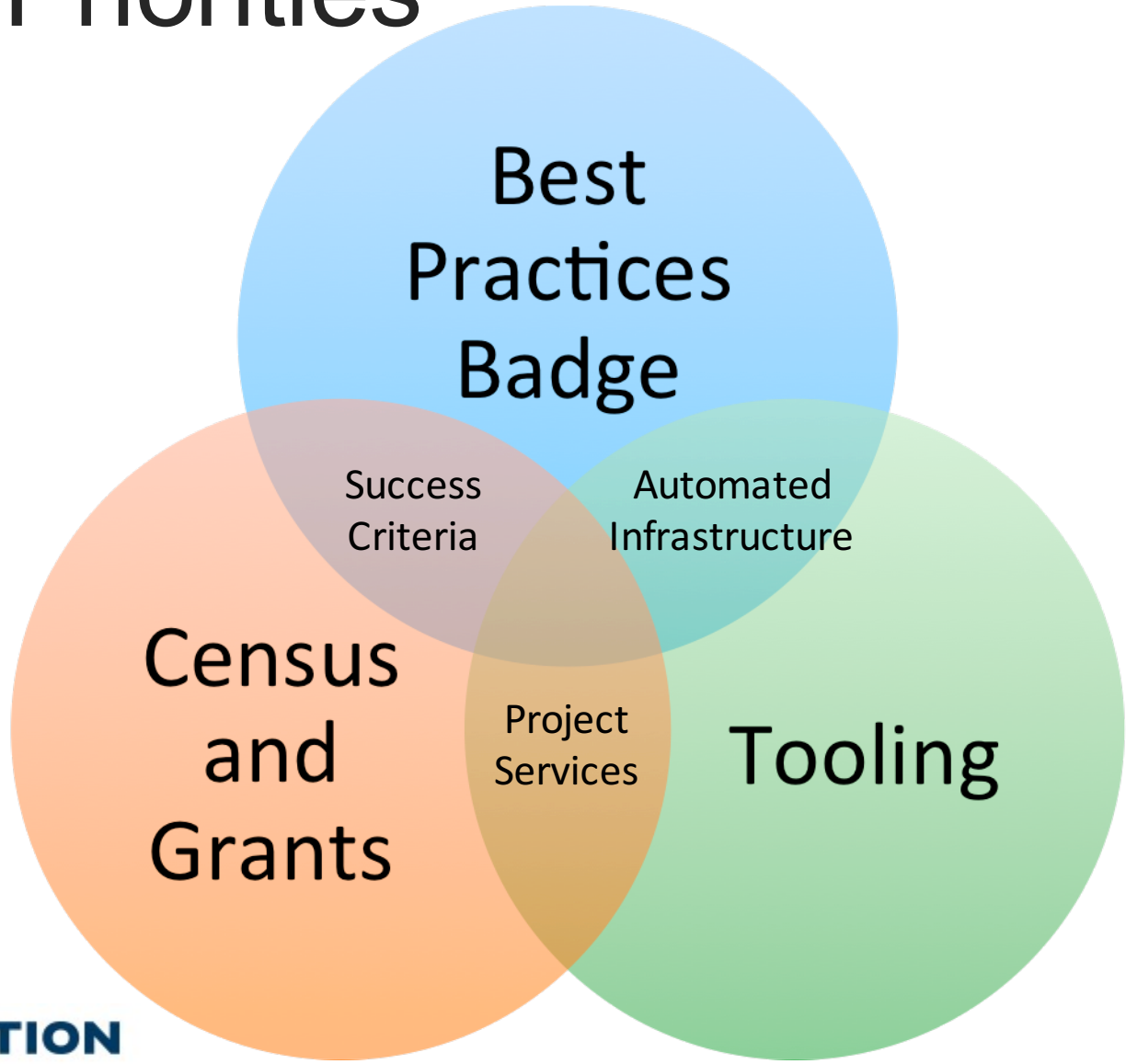
Agenda

- How CII got started
- How I got here
- What CII is doing
- Discussion about what comes next

Brief History of CII

- Founded April 24, 2014
- CII was founded as a direct reaction to the realization post-Heartbleed that OpenSSL was underfunded and that it wasn't the only critical open source project suffering this fate
- Mission – strengthen the open source upon which we all rely

CII 2015 Priorities



Grants

Core Infrastructure Initiative Grants

(All of this is on the coreinfrastructure.org website)

- OpenSSL
  - Funding for two developers
  - OpenSSL audit with Open Crypto Audit Project and NCC Group
- OpenSSH
  - Part time developer
  - Two years worth of bandwidth expenses
  - SSH Hackathon

Core Infrastructure Initiative Grants

- GnuPG
  - Part time developer
- Network Time Protocol
  - Part time developer for core ntpd
  - Part time developer for ntimed
  - Part time developers for NTPSec

Core Infrastructure Initiative Grants – Phase 2

- Reproducible Builds
  - Two part time developers
- The Fuzzing Project
  - Part time developer
- False Positive Free Checking with Frama-C
  - One developer

LINUX FOUNDATION

Census

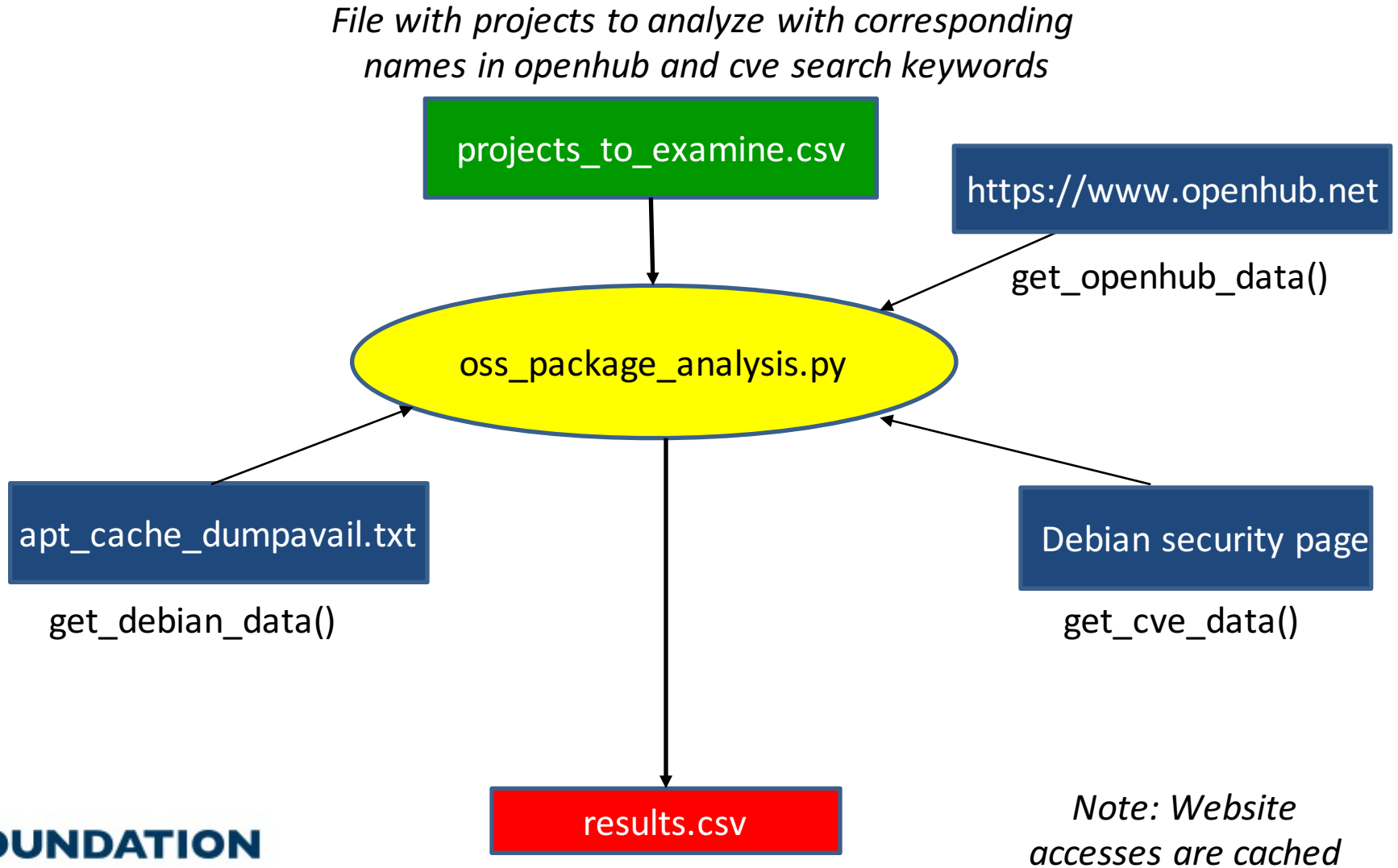
CII Census

- Which open source software packages need help?
  - Drowning in data
- Time to call for help from the luminary in the field of quantitative analysis of open source software and quantitative security metrics – David A. Wheeler

- What criteria indicate open source project strength on a relative scale?
  - Tens of criteria considered

Read the paper!

Analysis Process



Riskiest Projects (by score) (A snapshot in time)

Binary package name	Source package name (if different)	Score
ftp	netkit-ftp	11
netcat-traditional	netcat	11
tcpd	tcp-wrappers	11
whois		11
at		10
libwrap0	tcp-wrappers	10
traceroute		10
xauth		10
bzip2		9
hostname		9
libacl1	acl	9
libaudit0	audit	9
libbz2-1.0	bzip2	9
libept1.4.12	libept	9
libreadline6	readline6	9
libtasn1-3		9
linux-base		9
telnet	netkit-telnet	9

Score of currently funded projects

Project	Score
OpenSSL	8
Bash	6
GnuPG	7
NTPd	7
OpenSSH	8

Projects needing further review

- bzip2 (9)
- gzip (7)
- expat (libexpat1) (7)
- zlib (zlib1g) (7)
- libjpeg8 (7)
- libpng (libpng12-0) (7)
- unzip (7)
- mod-gnutls (libapache2-mod-gnutls) (8)

Example Findings

- netkit-ftp
- https://sources.debian.net/src/netkit-ftp/0.17-33/README/

Future plans for netkit maintenance are still up in the air, but in the meantime new releases will still appear from time to time. I don't have a whole lot of cycles to spare to work on netkit, so things are likely to continue to be fairly slow.

David A. Holland 23 July 2000

What should we do now?

Review and refine Census results

Retire

Revitalize

Replace

LINUX FOUNDATION

Best Practices Badge

CII Badge Program - Problem Statement

- Industry perspective:
  - When your developers want to use an open source project (or any third party code), how do you know how much risk that adds to the product?
- Open Source Developer perspective:
  - How do you know that the libraries and other projects that your project depends upon are being well maintained?

CII Badge Program

- CII Best Practices badge means that a project is serious about security
- Combination of automatically testable assertions and a questionnaire
- Language and framework-specific questions
- Applicable to both small and big projects, because the next big project will start small
- Free program; open source community to evolve criteria
- Allow for “compensating controls” rather than a strictly mechanical process

CII Badge Program – Example Criteria

- Basic OSS Practices
  - Project website
  - OSS license
- Change control
  - Source repository
  - Changelog
- Quality
  - Working build system
  - Automated test suite
  - New tests added when new functionality is added
- Security
  - Secured delivery mechanism
- Security analysis
  - Use of static and dynamic analysis

CII Badge Program – What's Next?

- Initial criteria on github
  - https://github.com/linuxfoundation/cii-best-practices-badge
- Discussion and pull requests welcomed
- Code development now starting
- Program launch after consensus reached around criteria and pilot code in place

LINUX FOUNDATION

Discussion Topics

What other core infrastructure projects would benefit from a grant?

“I would love to have a "security maintainer" whose job it is to review patches for security implications; nobody really does that now.”

--Anonymous

How do we revitalize dead packages?

Can students help?

What tools would help you do your job?

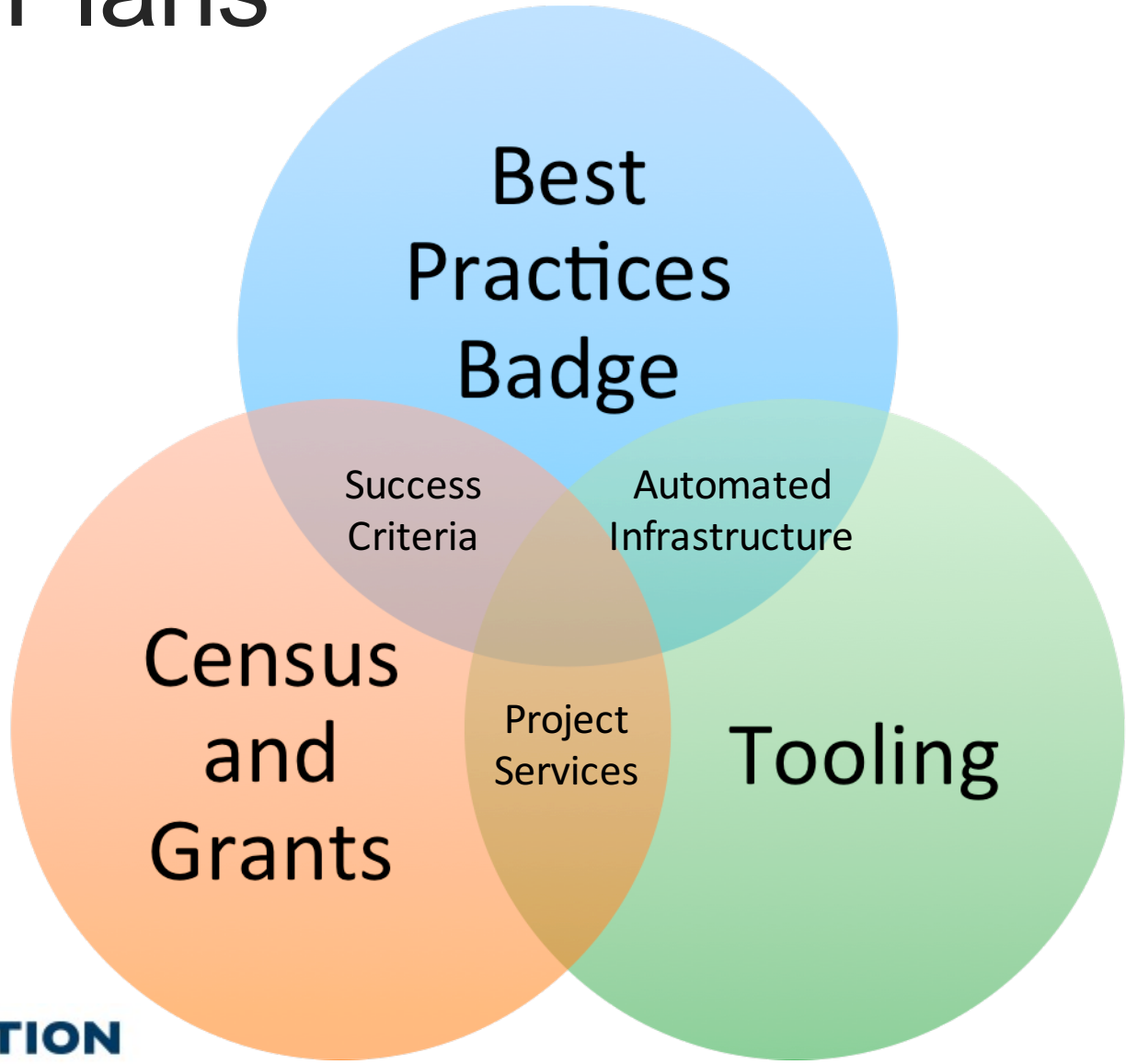
LINUX FOUNDATION

Thank you!

#cii on oftc

eratliff at linuxfoundation dot org

CII 2015 Plans



Current algorithm

- Project has website (1 if no)
- Written in C or C++ (2 if yes)
- CVE vulnerability reports: 3 points if 4+ , 2 points for 2-3, 1 point for 1.
- 12 month contributor count: 5 points for 0 contributors, 4 points for 1-3 contributors, 2 points if the number is unknown.
- Top 1% or 5% most popular Debian package: 2 or 1 if yes
- Exposure values: 2 points if directly exposed to the network (as server or client), 1 point if it is often used to process data provided by a network, and 1 point if it could be used for local privilege escalation.
- Application data only: *Subtract* 3 points if the Debian database reports that it is “Application Data” or “Standalone Data” (not an application)