



Open and secure: present and future

Making the UK and Europe a Safer Place to Work and Live Online

Mike Bursell
Chief Security Architect, Red Hat
2018-01-12

Agenda

- A little history
- The present
 - Open source
 - Open source and security
- The future
- Questions

And an apology

The title says “Open and secure”

There is no “secure”.

But we all know that, or we wouldn't be here anyway, right?

A little history

What is open source?

Open-source software (OSS) is computer software with its source code made available with a license in which the copyright holder provides the rights to study, change, and distribute the software to anyone and for any purpose.

https://en.wikipedia.org/wiki/Open-source_software

What is open source?

Open source isn't nerdy teenage boys coding in their
parents' basements anymore

What is open source?

Open source isn't *just* nerdy teenage boys coding in their
parents' basements anymore

Contributors to Linux kernel (an example)

2015-2016

Company	Changes	Percent of total
Intel	14,384	12.9%
Red Hat	8,987	8.0%
None	8,571	7.7%
Unknown	7,582	6.8%
Linaro	4,515	4.0%
Samsung	4,338	3.9%
SUSE	3,619	3.2%
IBM	2,995	2.7%
Consultants	2,938	2.6%
Renesas Electronics	2,239	2.0%

<https://www.linux.com/blog/top-10-developers-and-companies-contributing-linux-kernel-2015-2016>

Contributors to Linux kernel (an example)

2015-2016

Company	Changes	Percent of total
Intel	14,384	12.9%
Red Hat	8,987	8.0%
None	8,571	7.7%
Unknown	7,582	6.8%
Linaro	4,515	4.0%
Samsung	4,338	3.9%
SUSE	3,619	3.2%
IBM	2,995	2.7%
Consultants	2,938	2.6%
Renesas Electronics	2,239	2.0%

Yay!



redhat®

<https://www.linux.com/blog/top-10-developers-and-companies-contributing-linux-kernel-2015-2016>

Who is Red Hat?

(And who am I?)

“Red Hat is the world's leading provider of open source software solutions”

- Founded 1993
- Dec. '18 quarterly revenue \$748 million, annual revenues > \$2 billion
- Approximately 12,000 employees
- *Not* just Linux
 - Cloud, middleware, storage, virtualisation, management, etc.

Me:

- Chief Security Architect
- report directly to our CTO
- also own blockchain technical strategy for Red Hat

Is open source less secure than proprietary?

An old chestnut

No.

Is open source less secure than proprietary?

An old chestnut

No.

1. (Almost) no software is perfect.
2. There is good proprietary software.
3. There is bad Open Source software.
4. There are some very clever, talented and devoted people who create proprietary software.
5. The pool of people available to write and improve proprietary software is limited, even within the public sector and government realm.
6. The corresponding pool of people for Open Source is virtually *unlimited*...
7. ...and includes a goodly number of the talent pool of people writing proprietary software.
8. Public sector and government organisations often open source their software anyway.
9. There are businesses who will support Open Source software for you.
10. Contribution - even usage - adds to the commonwealth.

Is open source less secure than proprietary?

An old chestnut

No.

1. (Almost) no software is perfect.
2. There is good proprietary software.
3. There is bad Open Source software.
4. There are some very clever, talented and devoted people who create proprietary software.
5. The pool of people available to write and improve proprietary software is limited, even within the public sector and government realm.
6. The corresponding pool of people for Open Source is virtually *unlimited*...
7. ...and includes a goodly number of the talent pool of people writing proprietary software.
8. Public sector and government organisations often open source their software anyway.
9. There are businesses who will support Open Source software for you.
10. Contribution - even usage - adds to the commonwealth.

The question people are really asking is usually:

“Is unsupported open source software less secure than supported proprietary software?”

To which the answer is... “sometimes.”

The present: Open source

Who uses open source?

And what for?

- Pretty much everybody:
 - Financial, defence, government, manufacturing, healthcare, academia, ...
- Cloud
 - at least 40% of Microsoft Azure VMs are Linux (Oct '17)
- Internal servers
- Little desktop
 - (unless you count Android tablets)
- Linux has replaced old UNIX for business-critical workloads
- Many middleware frameworks are open source

Using open source

Maintenance, support

What changed?

- Linux matured
- Commercial support became real
- Consortia provided governance and structure

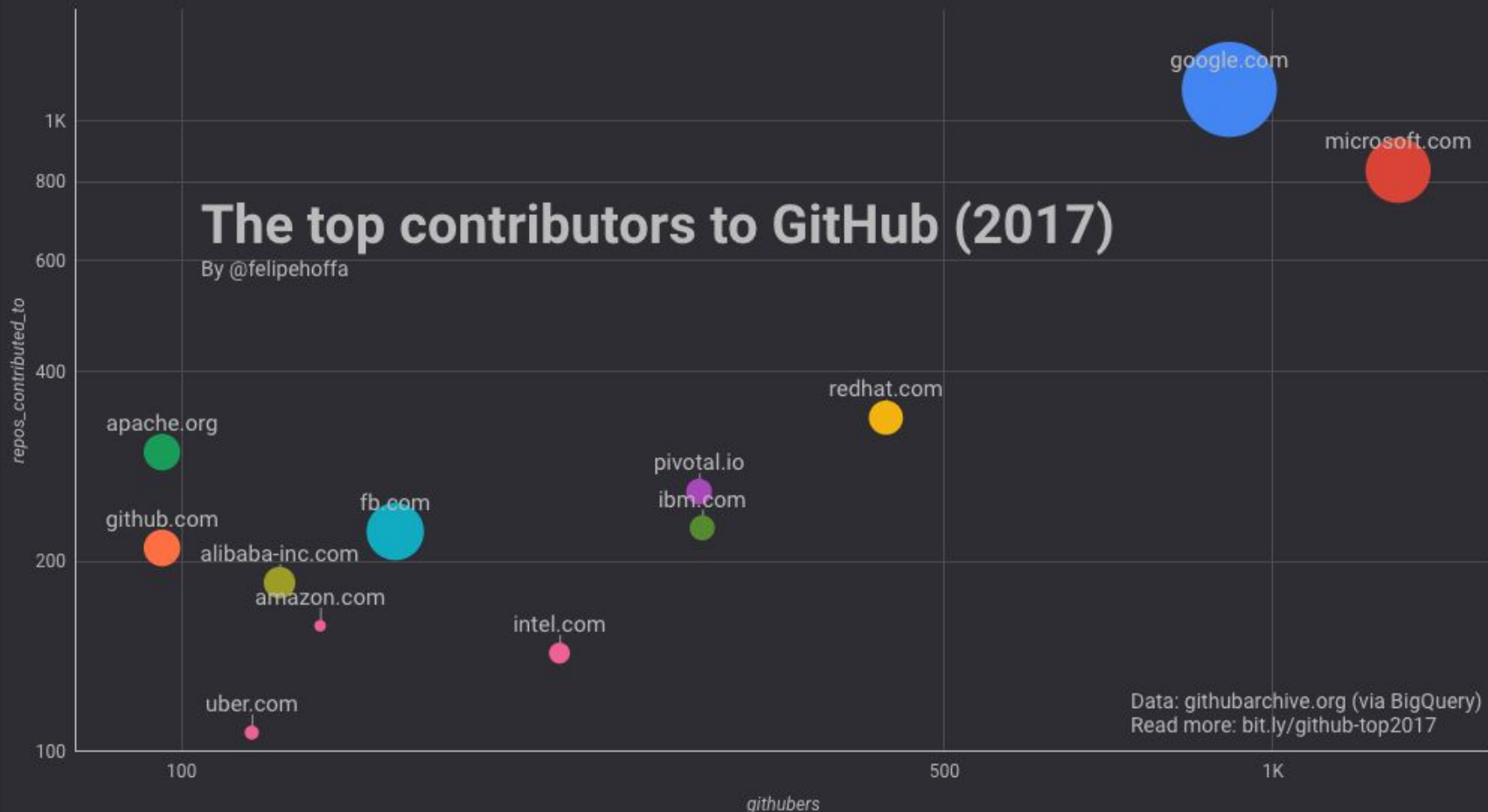


The top contributors to GitHub (2017)

By @felipehoffa

repos_contributed_to

githubers



Data: githubarchive.org (via BigQuery)
Read more: bit.ly/github-top2017

Influence

Corporations get to use and influence software

Multi-nationals and governments

- Can see what they're running
- Can influence features
- Can help fix bugs

Influence & control

Corporations get to use and influence software

Multi-nationals and governments

- Can see what they're running
- Can influence features
- Can help fix bugs
- Can buy maintenance
 - And/or maintain for themselves

Influence & control

Corporations get to use and influence software

Multi-nationals and governments

- Can see what they're running
- Can influence features
- Can help fix bugs
- Can buy maintenance
 - And/or maintain for themselves

Visibility AND maintenance = reduced risk

- security is how it's delivered

The present: Open source and security

The many eyes fallacy

Open source and cryptography

- “With enough eyes, all bugs are shallow”
 - Difficult to find sufficient eyes which are:
 - Expert
 - Motivated
 - Non-partisan

The many eyes fallacy

Open source and cryptography

- “With enough eyes, all bugs are shallow”
 - Difficult to find sufficient eyes which are:
 - Expert
 - Motivated
 - Non-partisan
- Peer review of code is vital
 - Impact of mistakes can be:
 - Catastrophic
 - Long-lived
 - Difficult to remedy
 - Intentional...

● <https://aliceevebob.wordpress.com/2017/04/04/disbelieving-the-many-eyes-hypothesis/>

The backdoor argument

And open source

Any backdoor available to governments / law enforcement is available to criminals

The backdoor argument

And open source

Any backdoor available to governments / law enforcement is available to criminals

	Option	Outcomes
1	Rig the protocol	<ol style="list-style-type: none">1. Nobody sensible uses closed protocols.2. Rigged open protocols get noticed - specifications <i>are</i> checked.
2	Backdoor the software	Open source is visible. It may take a while, but people will notice.
3	Hand over keys	An operator issue. But how many sets for how many governments / LEAs?
4	Force use of “crippled” software	The bad folks will always use the uncrippled version.

- <https://aliceevebob.com/2017/07/11/that-backdoor-fallacy-revisited-delving-a-bit-deeper/>
- <https://aliceevebob.com/2017/03/27/the-backdoor-fallacy-explaining-it-slowly-for-governments/>

The commonwealth of open source

Assertion: use of open source software is a net benefit to the community

- Even non-contributors add to momentum
 - Those paying for maintenance contribute by proxy
- Coding is not the only type of contribution
 - Testing, reporting, documentation, marketing, evangelism, ...

The future

Changing models - it's not just software

Open source software is where it started, but there's more...

Changing models

Consumption





- Cloud usage and DevOps are changing how people consume software
 - Images and provenance
 - Auto-update
 - The “Smaug problem” - or “over-enthusiastic developers”
- *aaS hides lower layers
 - ✓ • less to worry about
 - ✓ • concentrate on your expertise
 - ✗ • decreased control
 - ✗ • decreased visibility

Changing models

Consumption

- Cloud usage and DevOps are changing how people consume software
 - Images and provenance
 - Auto-update
 - The “Smaug problem” - or “over-enthusiastic developers”

- *aaS hides lower layers

-  • less to worry about
-  • concentrate on your expertise
-  • decreased control
-  • decreased visibility

Question: what's the correct amount of openness? And to whom?

Consider the Meltdown & Spectre issues:

- Chip vendors
- OS vendors
- Cloud Service Providers
- In-house teams

Changing models

Data

- Open Data is becoming widespread
- How would be expand even further?
 - Share data from automated vehicles, logistics companies, performance metrics, home automation...
 - Expose aggregated data more safely
 - Multi-party computation (MPC) and Differential Privacy techniques offer some possibilities
- Think of data as part of the commonwealth

Changing models

Applications

New technologies, new ways of doing business.

- Blockchain
- AI
- “The cloud”
- Serverless

We are seeing a “default to open”.

Changing models

Applications

New technologies, new ways of doing business.

- Blockchain
- AI
- “The cloud”
- Serverless

We are seeing a “default to open”.

And that’s a good thing.

Questions

<https://aliceevebob.com> - my blog

<https://www.linkedin.com/in/mikebursell/>

@MikeCamel

MikeCamel





THANK YOU



plus.google.com/+RedHat



facebook.com/redhatinc



linkedin.com/company/red-hat



twitter.com/RedHatNews



youtube.com/user/RedHatVideos