So you’ve always wanted to be an Mbed TLS reviewer?

Dave Rodgman
2020-11-03

I always wanted to be… an astronaut?

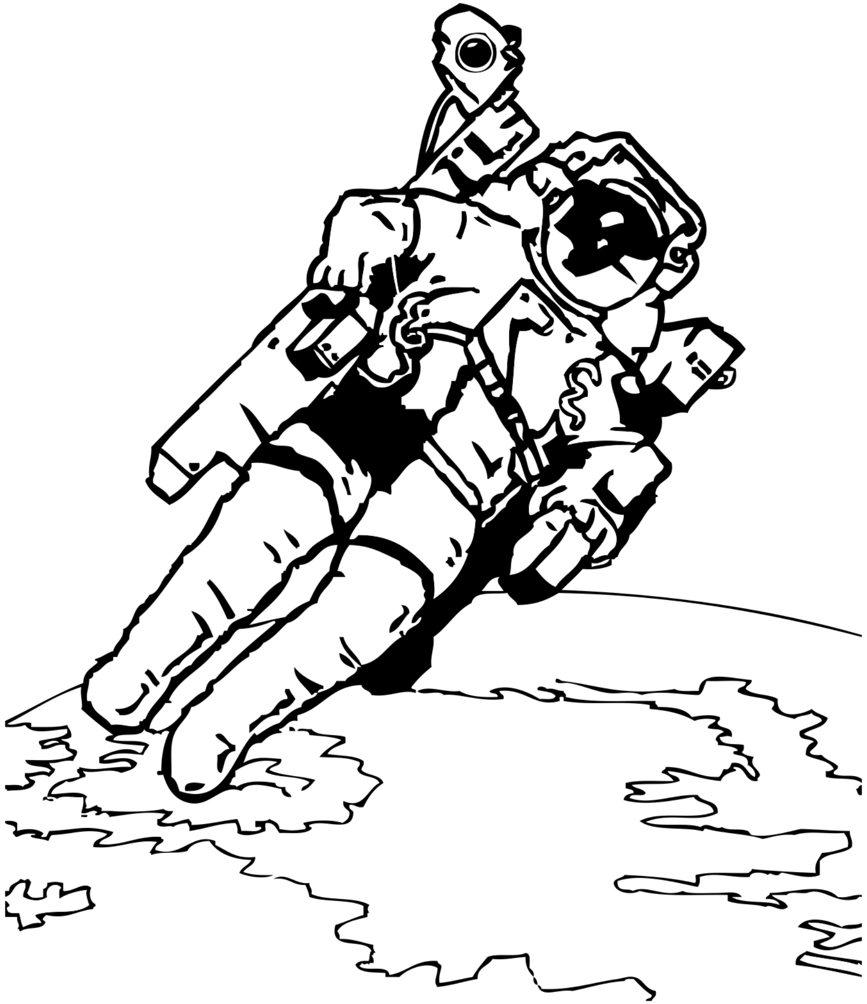


Image: https://pixabay.com/vectors/astronaut-space-walk-spacewalk-31069/

I always wanted to be… an athlete?

Image: https://iconscout.com/icons/soccer by Christian Mohr

I always wanted to be… an MbedTLS reviewer!

Image: https://pixabay.com/photos/accountant-programmer-guys-joy-2252316/

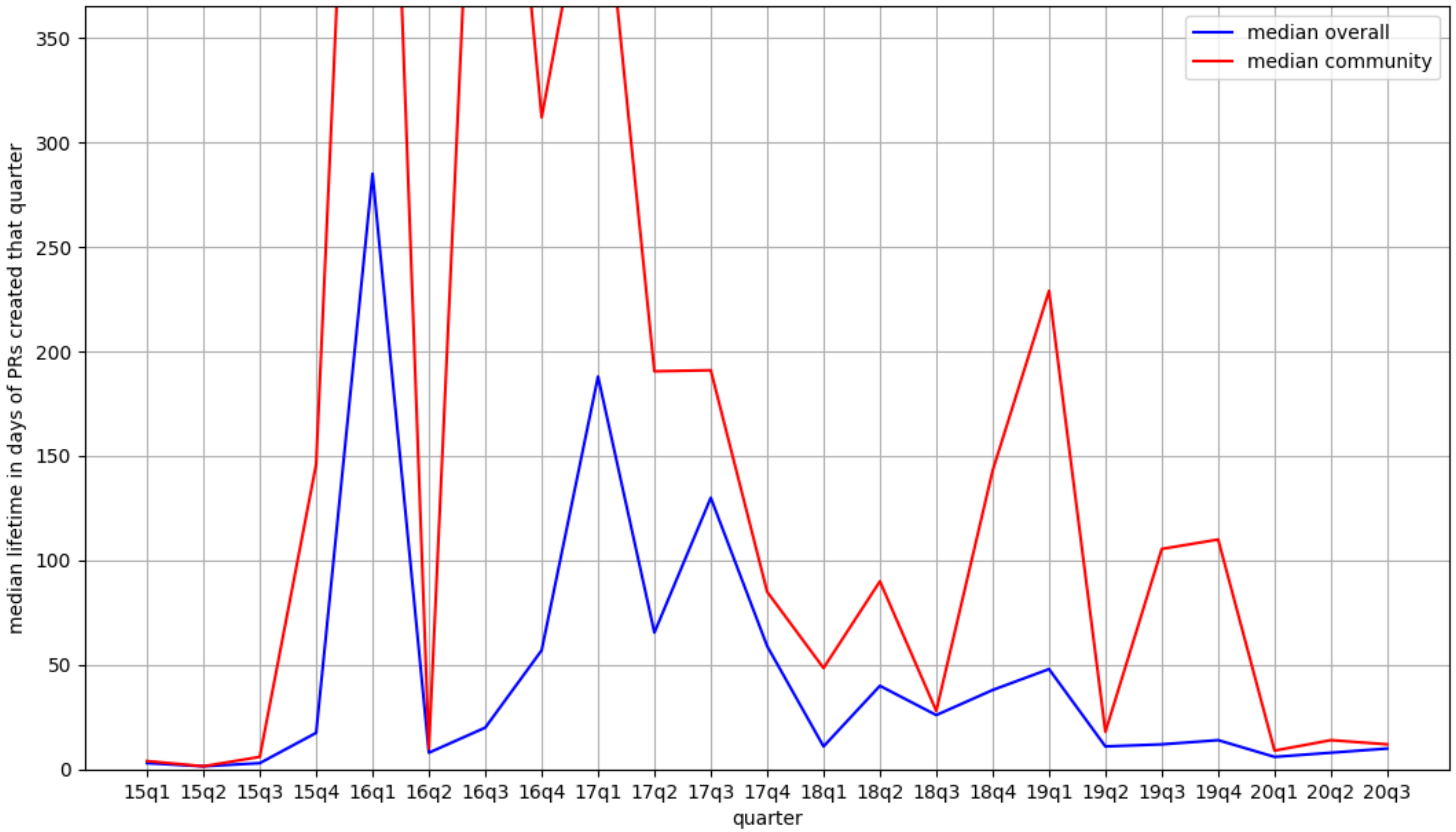
Agenda

- Background: we’re keen to get external reviewers
- How to progress towards becoming an “official” reviewer
- How to conduct a great review

Background

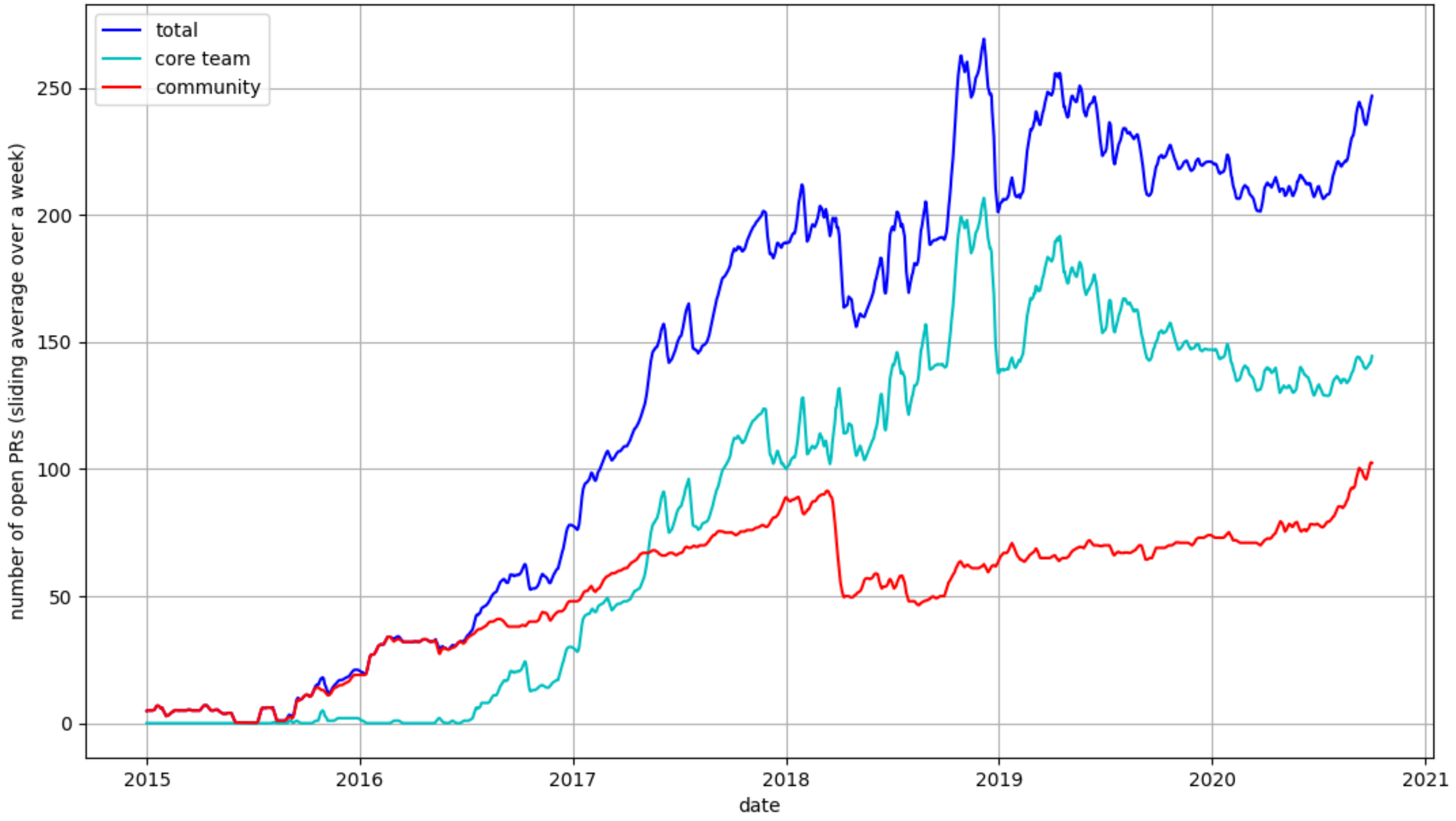
The current state of play: we're responsive…

Median lifetime of PRs per quarter (less is better)

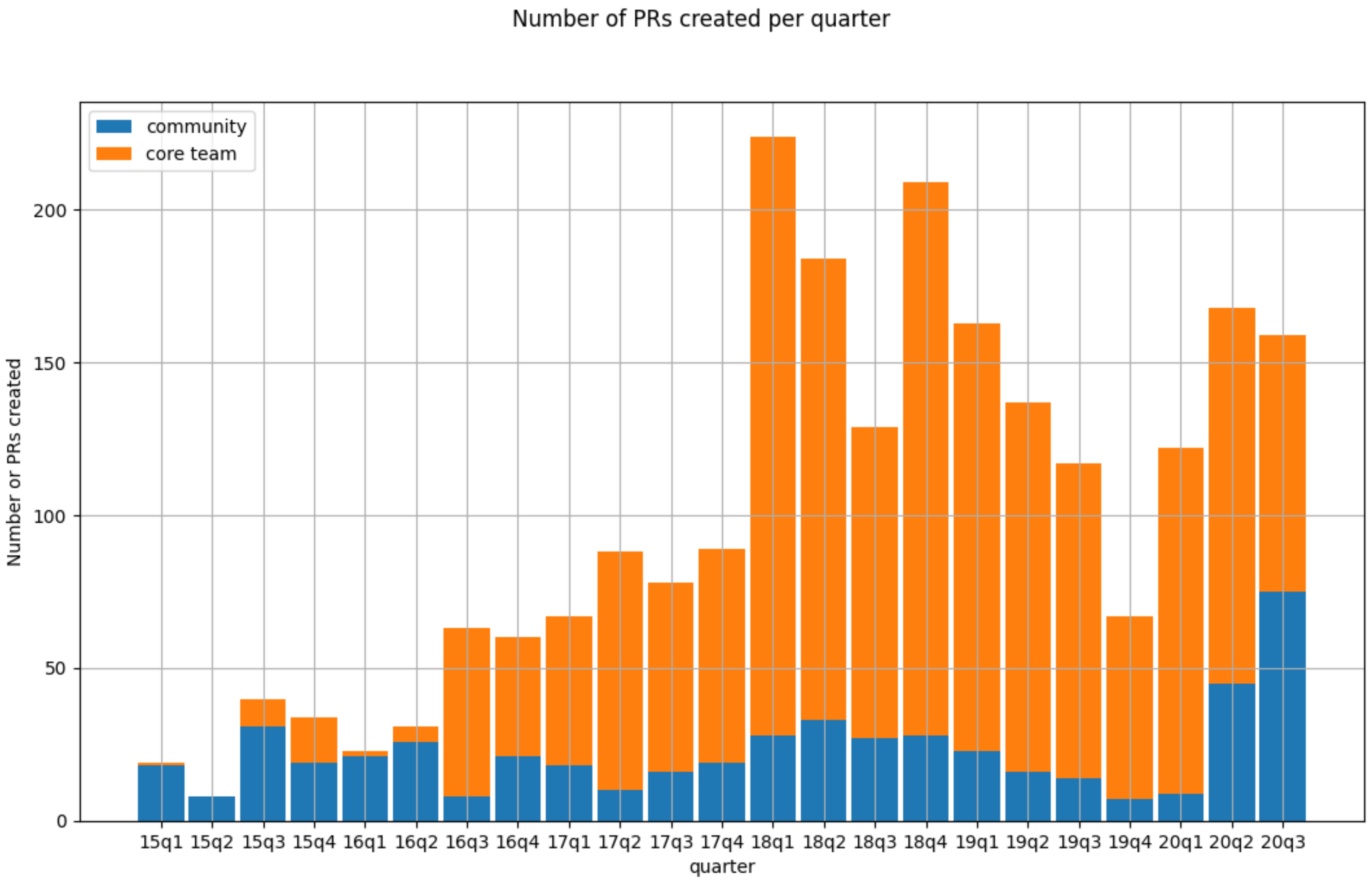


The current state of play: ... but the workload is going up

Number of PRs pending over time (less is better)



The current state of play: … but the workload is going up



Security libraries are tricky

- Bugs don’t just mean crashes
  - They may invisibly weaken security
  - Not possible to catch with tests!

- People may be actively trying to backdoor the project
  - Example (Linux kernel, 2003): https://lwn.net/Articles/57135/

- Some PRs may be very complex and require deep maths / crypto knowledge to understand
  - Not all reviewers / maintainers will have right skills to review every PR – that’s OK

The story so far

- Every PR must have approval from two “official” reviewers
  - Reviews from other people help and are welcome, but don’t formally count
- Currently, all official maintainers and reviewers are Arm employees
  - We do have reviewers who don’t formally work on the project (ex-project members)
- SiliconLabs are regularly contributing reviews
- David Brown @Linaro working towards becoming a reviewer
- Other external reviews from time to time

How can we know when someone is ready to be a reviewer?

- We (existing maintainers) need to be confident that the person is
  - Competent
  - Trustworthy

- Competence
  - Shown through submitting good PRs and good reviews

- Trustworthiness
  - Very tricky
  - Two-reviewer system provides a backstop

- The challenge for us: support external people on this path

Steps to becoming a reviewer

Practical roadmap to becoming a reviewer

- Submit some PRs
  - No fixed size or number
  - Can start small & progress to more complex areas

- Start contributing reviews
  - Two additional “official” reviewers are still required
  - But there is still lots of value in contributing good reviews!

- No fixed targets!
  - Should have made “some significant contributions”
  - Could be as a reviewer only, but would expect normally people will start with PRs
  - Significant period of time (three months+) to demonstrate experience with the project

Becoming an official reviewer

- A proposer (existing maintainer/reviewer) proposes you as a reviewer
- A seconder (existing maintainer/reviewer) must support the nomination
- If there is general support / no disagreement, the nomination will be accepted

- This is a new process – might refine it with time

The most important step

- People often don’t feel confident contributing reviews at first
  - True even for new people within the MbedTLS team
  - Fear of “not being ready”, etc.

- Only solution is to **contribute some reviews**!
  - We will be supportive & happy to see community reviews
  - If there are questions, we can answer them via the mailing list

- Where do I start?
  - All open issues
    https://github.com/ARMmbed/mbedtls/pulls?q=is%3Apr+is%3Aopen
  - Open, good first issue (simple PRs)
    https://github.com/ARMmbed/mbedtls/pulls?q=is%3Apr+is%3Aopen+label%3A%22Good+first+issue%22

How to conduct a great review

Some technical notes on review

- Coding standards can be found here
  - https://tls.mbed.org/kb/development/mbedtls-coding-standards

- Following other reviews is a good way to understand what kind of things reviewers will often look for

- We plan to publish further documentation on the review process

High-level review guidelines

- Gilles Peskine has given a previous talk on this subject
  https://developer.trustedfirmware.org/w/mbed-tls/processes/review/

- TLDR:
  - Look at the PR from many angles: gatekeeper, maintainer, user, attacker, competitor, …
  - Think about the worst-case scenario
  - Remember you are taking responsibility for the quality of the PR…
  - … but don’t panic – the second reviewer will help ensure a thorough job is done

arm

Thank You

Danke

Merci

谢谢

ありがとう

Gracias

Kiitos

감사합니다

धन्यवाद

شكرًا

ধন্যবাদ

תודה