April 24, 2021

An open letter to the Linux community

Dear Community Members:

We sincerely apologize for any harm our research group did to the Linux kernel community. Our goal was to identify issues with the patching process and ways to address them, and we are very sorry that the method used in the “hypocrite commits” paper was inappropriate. As many observers have pointed out to us, we made a mistake by not finding a way to consult with the community and obtain permission before running this study; we did that because we knew we could not ask the maintainers of Linux for permission, or they would be on the lookout for the hypocrite patches. While our goal was to improve the security of Linux, we now understand that it was hurtful to the community to make it a subject of our research, and to waste its effort reviewing these patches without its knowledge or permission.

We just want you to know that we would never intentionally hurt the Linux kernel community and never introduce security vulnerabilities. Our work was conducted with the best of intentions and is all about finding and fixing security vulnerabilities.

The “hypocrite commits” work was carried out in August 2020; it aimed to improve the security of the patching process in Linux. As part of the project, we studied potential issues with the patching process of Linux, including causes of the issues and suggestions for addressing them.

- This work did not introduce vulnerabilities into the Linux code. The three incorrect patches were discussed and stopped during exchanges in a Linux message board, and never committed to the code. We reported the findings and our conclusions (excluding the incorrect patches) of the work to the Linux community before paper submission, collected their feedback, and included them in the paper.
- All the other 190 patches being reverted and re-evaluated were submitted as part of other projects and as a service to the community; they are not related to the “hypocrite commits” paper.
- These 190 patches were in response to real bugs in the code and all correct--as far as we can discern--when we submitted them.
- We understand the desire of the community to gain access to and examine the three incorrect patches. Doing so would reveal the identity of members of the community who responded to these patches on the message board. Therefore, we are working to obtain their consent before revealing these patches.
- Our recent patches in April 2021 are not part of the “hypocrite commits” paper either. We had been conducting a new project that aims to automatically identify bugs introduced by other patches (not from us). Our patches were prepared and submitted to fix the identified bugs to follow the rules of Responsible Disclosure, and we are happy to share details of this newer project with the Linux community.

We are a research group whose members devote their careers to improving the Linux kernel. We have been working on finding and patching vulnerabilities in Linux for the past five years. The past observations with the patching process had motivated us to also study and address issues with the patching process itself. This current incident has caused a great deal of anger in the Linux community toward us, the research group, and the University of Minnesota. We apologize unconditionally for what we now recognize was a breach of the shared trust in the open source community and seek forgiveness for our missteps.

We seek to rebuild the relationship with the Linux Foundation and the Linux community from a place of humility to create a foundation from which, we hope, we can once again contribute to our shared goal of improving the quality and security of Linux software. We will work with our department as they develop new training and support for faculty and students seeking to conduct research on open source projects, peer-production sites, and other online communities. We are committed to following best practices for collaborative research by consulting with community leaders and members about the nature of our research projects, and ensuring that our work meets not only the requirements of the IRB but also the expectations that the community has articulated to us in the wake of this incident.

While this issue has been painful for us as well, and we are genuinely sorry for the extra work that the Linux kernel community has undertaken, we have learned some important lessons about research with the open source community from this incident. We can and will do better, and we believe we have much to contribute in the future, and will work hard to regain your trust.

Sincerely,

Kangjie Lu, Qiushi Wu, and Aditya Pakki
University of Minnesota