This is Kaiming from PSU,  I’m a PhD candidate working with Trent Jaeger in the system security area. Now I am pleased to nominate the paper titled "Progressive Scrutiny: Incremental Detection of UBI bugs in the Linux Kernel" for the Annual Best Scientific Cybersecurity Paper Competition. This paper is a significant contribution to the field of cybersecurity science, introducing an innovative approach to detect and track the evolution of bugs in the Linux Kernel through incremental static analysis.

The paper is accepted in NDSS 2022 and it is the first to conduct a large-scale experiment that incrementally analyzes the Linux Kernel. It uses the use-before-initialization (UBI) bugs, which are considered one of the most severe security vulnerabilities in the Linux kernel, to showcase the effectiveness and speedup of the incremental analysis. The paper also provides a comprehensive evaluation of the proposed technique by analyzing about fifty versions of the Linux Kernel.

The contributions of the paper are significant for several reasons. Firstly, the Linux kernel is widely used in operating systems and deployed in millions of systems worldwide, including servers that operate 24 hours a day, making its security of paramount importance. Additionally, with over 27 million lines of code and an average of 10 commits per hour, ensuring the security of the Linux Kernel is a big challenge. A scalable testing approach that fits into the development cycle is urgently needed for security purposes. The paper addresses this challenge by proposing an incremental method that reduces the analysis time and resources required to detect bugs by reusing invariants from previous kernel properties.

Secondly, the paper provides empirical evidence of the proposed technique's effectiveness by using UBI bugs as a case study and analyzing about fifty versions of the Linux Kernel. The results show that the proposed technique can detect almost all bugs found by the traditional clean slate approach in significantly less time, making it a valuable addition to the field of cybersecurity science. Besides, the kennel community has accepted new patches submitted by them.

Finally, the proposed approach can also help developers differentiate between security patches and normal commits, reducing the time to fix bugs and the threats a bug could introduce.

In conclusion, the paper titled "Progressive Scrutiny: Incremental Detection of UBI bugs in the Linux Kernel" is a deserving nominee for the paper competition. It presents a novel approach that contributes significantly to the advancement of cybersecurity science and has impacted the field positively.

Sincerely,

Kaiming