

Call for nominations: *NSA invites nominations of papers that show an outstanding contribution to cybersecurity science. Nominations include, in 500 words or less, a nomination statement describing the scientific contribution of the paper and explaining why this paper merits the award. Considerations in evaluating the nominated paper include: Scientific merit and significance of the work reported, and the degree to which the paper exemplifies how to perform and report scientific research in cybersecurity.*

Nomination

This paper presents a groundbreaking foundational contribution to fuzzing, a technique widely recognized as the most effective method for automated bug finding and utilized by major organizations such as Google, Microsoft, and Facebook. Despite its critical role in secure software development, the design of new fuzzers lacks a guiding theoretical framework, relying mainly on intuitions and empirical results.

This paper, for the first time, introduces a new theoretical framework (based on computational complexity) for designing the next generation of fuzzers, which represents a major breakthrough in the field. This framework provides a more rigorous and principled method for fuzzing, overcoming limitations of existing research and establishing a new foundation for scientific exploration in the area.

The paper's three key contributions demonstrate the scientific significance of the work.

1. It provides a theoretical performance metric based on computational complexity theory that offers a more comprehensive assessment of fuzzer performance. This metric is a significant improvement over ad hoc metrics currently used to evaluate fuzzers and allows for a more rigorous comparison of different fuzzing techniques.
2. It proves a lower bound on the performance of any fuzzer, which is a difficult task given the need to reason about all possible future fuzzers. This is a significant theoretical result that has important implications for the design and optimization of fuzzers.
3. It presents the design of an asymptotically optimal fuzzer as well as an implementation that outperforms existing state-of-the-art fuzzers by an unprecedented factor (e.g., two orders of magnitude). Such results are a testament to the power of their theoretical approach and demonstrate the potential for a new generation of fuzzers based on this approach.

In addition to these contributions, the paper is notable for its clarity and accessibility. Despite the complexity and novelty of the approach, the authors present their ideas in a clear and concise manner, making the paper accessible to a wide audience. This clarity and accessibility have contributed to the paper's success, as major industry players are eager to incorporate the authors' insights into their secure software development practices.

In summary, the paper represents a major advance in fuzzing. It sets a new standard for how to perform and report scientific research in fuzzing. In addition, it offers a new theoretical framework for designing more effective fuzzers, demonstrating the kind of theoretical innovation that can potentially transform a field. For these reasons, it is a highly deserving nominee for the NSA's award.