Software Engineering Seminar

Finding Exploits with Symbolic Execution

Description

Exploits in software systems may pose big safety and security risks. Naturally, (automated) techniques to detect existing exploits are necessary to ensure the well-behaviour of software systems. In this context, *symbolic execution*, as used in [1], can be a powerful tool to recognize exploits.

The student is to examine and discuss the approach given in the paper and compare it with similar techniques.

References

[1] Sang Kil Cha, Thanassis Avgerinos, Alexandre Rebert, and David Brumley. Unleashing mayhem on binary code. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, SP '12, pages 380–394, Washington, DC, USA, 2012. IEEE Computer Society.

Contacts

Simon Heiden (`heiden@informatik.hu-berlin.de`)
Software Engineering Group
Institut für Informatik
Humboldt-Universität zu Berlin