Contribution ID: **4** Type: **not specified**

Defeating Encryption By Using Unicorn Engine

Software Reverse-Engineering (SRE) is often considered black magic, but with the right tools and knowledge, its processes can be significantly accelerated. Unicorn Engine is a powerful framework that allows you to execute code platform-independently, which can greatly enhance your SRE skills.

Applications, binaries, and frameworks often contain complex functionalities like encryption and decryption methods that are hidden from the user. Reverse-engineering these can be difficult and time-consuming, especially when they involve non-standard, proprietary or non-documented cryptographic functions. This is where Unicorn Engine comes in. It enables us to execute code dynamically without the need for the proper environment or hardware. By emulating the execution, we can analyse and understand the underlying operations, making the reverse-engineering process more effective.

With Unicorn Engine, you can dissect and manipulate code in a controlled environment. Whether you are dealing with malware analysis, software debugging, or vulnerability research, Unicorn Engine is an awesome tool in your reverse-engineering toolkit.

This training will focus on reverse-engineering one or more binaries with Ghidra. Participants will identify various encryption or obfuscation functions and write code for Unicorn Engine in Python to utilise these functions without ever executing the binary.

No special knowledge is required, but familiarity with Python, Ghidra, and assembly would be beneficial. The training will introduce Unicorn Engine to the audience and explain it in depth.

Length

Half day

Optional: Speaker / convener biography

Balazs Bucsay is the founder & CEO of Mantra Information Security that offers a variety of consultancy services in the field of IT Security. With decades of offensive security experience, he is focusing his time mainly on research in various fields including red teaming, reverse engineering, embedded devices, firmware emulation and cloud. He gave multiple talks around the globe (Singapore, London, Melbourne, Honolulu) on different advanced topics and released several tools and papers about the latest techniques. He has multiple certifications (OSCE, OSCP, OSWP) related to penetration testing, exploit writing and other low-level topics and degrees in Mathematics and Computer Science. Balazs thinks that sharing knowledge is one of the most important things, so he always shares it with his peers. Because of his passion for technology, he starts the second shift right after work to do some research to find new vulnerabilities.

Primary author: BUCSAY, Balazs (CEO & Founder)

Track Classification: Workshops, training, tabletop games, hands-on exercises, birds of a feather sessions, etc.