

# Summary

ROPER is an genetic ROP-chain compiler. It uses evolutionary methods (natural selection) to develop specially crafted payloads called 'ROP-chains', which are used in cyber-attacks. These permit the attacker to gain control of a target process's execution, while leveraging that process's privileges.

A ROP-chain differs from a traditional shellcode attack in that it introduces no foreign code to the target process, and does not rely on being able to write to executable memory.

Instead, it hops around memory segments that have already been mapped as executable, assembling them into a sort of mosaic. This mosaic performs operations that the original program's author never intended.

ROPER spawns an entire population of such mosaics, randomly at first, and then uses the principles of natural selection to breed one that accomplishes *precisely* what the attacker desires, but using means the attacker, being human, would not have herself anticipated.

In fact, ROPER has already shown itself capable of performing subtle, adaptive tasks that ROP-chains – whether handmade or deterministically compiled – have never before been capable of, achieving over 95 % accuracy even when asked to classify Iris flowers, for example. This gives us a glimpse of the ROPER's capacity to dynamically adapt to problems for which it was not designed.