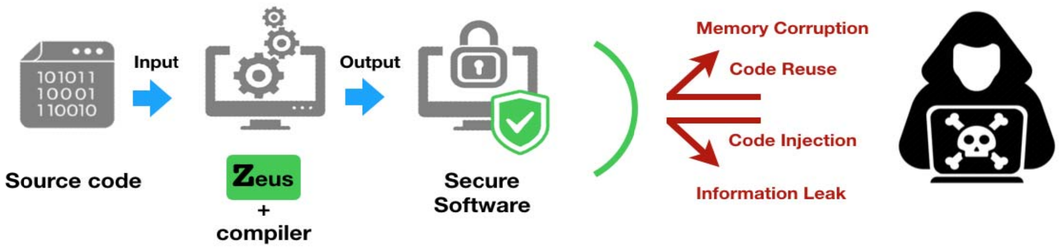
Zeus Software Defender Technology

Patented Zeus Software Defender Technology ("Zeus") is a tool for hardening C and C++ programs to provide shields for protecting against cybersecurity attacks.



Protecting computer memory is critical in software program security because most of the breaches in programs are related to memory. Particularly, adversaries can disclose or divert control-flow by overwriting code pointers. Zeus injects instructions into programs at compile time to harden them by encrypting and decrypting pointers at runtime. These cryptographic operations mitigate the vulnerability of *information leaks* and *control-flow interceptions*. Specifically, Zeus updates encryption states for return addresses at runtime (*dynamic reencryption*) to protect C and C++ software programs.

Zeus can successfully mitigate real world cybersecurity attacks reported in CVE (Common Vulnerabilities and Exposures). As examples, Zeus can block control-flow hijacking caused by a stack buffer overflow vulnerability CVE-2018-18409 in the open source TCPFLOW project (https://github.com/simsong/tcpflow/wiki); CVE-2018-17439 and CVE-2018-15671 of the HDF5 library (https://www.hdfgroup.org/downloads); and CVE-2013-2028 of Nginx web server leaking a return address byte-by-byte (https://www.rapid7.com/db/vulnerabilities/nginx-cve-2013-2028).

- **Zeus dramatically reduces the risks caused by buffer overflow and any code pointer attacks.**
- **Zeus is effective in defending against various attack instances and patterns as well as in performance.**
- **Zeus has low execution time overhead and does not require any additional security features outside of the program.**
- **Zeus can cover zero-day attacks against code pointers.**
- **Zeus can be implemented in C and C++ Compliers.**

For Zeus details, please contact Alex G. Lee (alexglee@zeusswdef.com).