

# Software Side-Channel Attacks Against Intel SGX Enclaves

CS 658 Research Paper

Colin Howes  
University of Waterloo  
200 University Ave. W  
Waterloo, ON N2L 3G1  
chowes@uwaterloo.ca

## ABSTRACT

Intel Software Guard Extensions is a hardware extension designed to allow legacy programs to run securely in a cloud environment when all software on the host machine is potentially untrusted.

- 1 INTRODUCTION
- 2 SOFTWARE SIDE-CHANNEL  
ATTACKS
- 3 INTEL SGX
- 4 ATTACKS AGAINST SGX  
ENCLAVES
- 5 COUNTERMEASURES
- 6 FUTURE DIRECTIONS
- 7 CONCLUSIONS