UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

MSc Seminar

Tuesday May 14, 2024, at 1:30PM, Reynolds 2224

Brandon Lit

"I'm regretting that I hit run": In-situ Assessment of Potential Malware

Advisor: Dr. Hassan Khan
Advisory: Dr. David Flatla

Abstract:

We conduct the first ever two-session controlled lab study (n=36) where participants are prompted to install real benign and malicious software on a standard Windows laptop. In the first session, we establish users' strategies by asking them to assess the threat from software without any instructions. In the second session, we repeat the experiment after introducing an "enhanced task manager" application with system process information like CPU usage, files accessed, and network destination country to understand their decision making with the knowledge of some attack indicators.

We measure the time and accuracy to classify software as benign or malicious and participant comments using a "think-aloud" protocol. The comments form a dataset of 2,651 excerpts that are coded into four top-level categories of "indicators" with 25 sub-categories. We employ the indicators to provide a perspective into how end-users examine and analyze software in-situ. Our results show end-users are surprisingly accurate at classifying malware and become even better when provided with the attack indicators.

Our analysis uncovers common misconceptions, shows reliance on indicators that are circumventable, and provides actionable insights for software and operating system providers to improve their interfaces or notifications.