

University of Toronto **Engineering**



UNIVERSITY OF TORONTO
FACULTY OF APPLIED SCIENCE & ENGINEERING

Module 13 – Reverse Engineering

Disassembly, patching and Trojan horses



UNIVERSITY OF TORONTO
FACULTY OF APPLIED SCIENCE & ENGINEERING

Module 13 – Reverse Engineering

Reverse engineering is changing compiled code

- It allows us to create a **Trojan horse** type of malware
- We can change a legitimate programme to do what we want!
- We can then distribute that programme to others
- We can also **crack** it: circumvent passwords and other authentication checks
- Let's try it!
 - *Run “secret.exe” in your shared folder*
 - *The password is “aRatherUnsecurePassword”*
 - *We'll look at the code to see where to patch the machine code...*
 - *... and to see where to alter it mid-execution*



[33]



Thanks!

Questions?

Email: b.graydon@ieee.org



UNIVERSITY OF TORONTO
FACULTY OF APPLIED SCIENCE & ENGINEERING