

# Reversing C++ code

*Applying our new found knowledge*

© Government of Canada

This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.



Communications  
Security Establishment

Centre de la sécurité  
des télécommunications

PAGE 1

Canada 

# Important note

*Every C++ compiler has it's own personality. The important part is the general concept of C++ reverse engineering.*

© Government of Canada

This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.



# **If you have IDA pro, now is the time to open it up!**

This will mostly be a demonstration but don't be afraid to ask questions.



# Reversing C++ using IDA Pro

- Take full advantage of the “struct” feature of IDA pro
- Don't forget to use base + displacement with the struct you built!
- Don't forget to demangle names...
- Don't forget you need 2 structs per class
  - One for the VTable
  - One for the class itself
  -

The rest, really is identical to reversing C code. You just need to get your head around the fact that the code will call functions in a bit of a different way.

