Reverse Engineering 101

Zach Wick
zwick on IRC
zach@zachwick.com

All Hands Active
http://allhandsactive.com

April 14, 2014

Agenda

- What is "Reverse Engineering"
- Legality of it all
- Compilation
- What the ELF?
- ELF soup
- Next Class
  - Bus Traffic
  - Oscilloscopes Gallore!
- Further Reading

What is "Reverse Engineering"?

"Analyzing the components of a system in order to ascertain how that system functions." - Zach Wick April 14, 2014

- Using
- Probing
- Disassembling (software term, hardware term)
- Reading documentation

Am I (Legally) Allowed to Do This?

- As long as you legally acquired the thing, probably
- Software EULA's have been found to trump copyright law (Bowers v. Baystate Technologies)
- DMCA Section 103(f)
  - Can RE and circumvent protection to achieve interoperability
- EFF Coders' Rights Project

Code Compilation

- Source Code
- Object Code

Compilation is what gets us from source to object code

What the ELF?

- Executable and Linkable Format
- executables, object code, shared libs, core dumps
- 1999 chosen as standard binary file format on x86 systems

Structure of an ELF

Further Reading

- https://en.wikipedia.org/wiki/Executable_and_linkable_Format
- https://en.wikipedia.org/wiki/Objdump
- https://en.wikipedia.org/wiki/Reverse_engineering
- https://www.eff.org/issues/coders