Reverse Engineering 101

 \mathbf{n} \mathbf{n} a m a m a u



- Humans do not so we use programming languages
- "Low level = close to metal" and "high level = easy to code"
- Programs are complied and then used
- This is where reverse engineering comes in.. Making binaries jump

n a m a m а



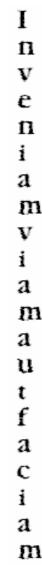
- People believed that once code was compiled it was safe
- Compiling code to binary was seen as type of encryption
- So compiling was used to "hide" algorithms, data, etc
- So if you could "see" or deduce the code from the binary...
- ...well you could make the program do what you wanted
- This is was the goal behind the underground RE, to "crack" games, etc

 \mathbf{n} a m a m а



"Who? Why?"

- Underground
 - To crack software
 - To gain proprietary information
 - To find vulnerabilities
- Government
 - Verifying trust in used software/hardware
 - To gain proprietary information
- Companies
 - To crack software
 - To gain proprietary information
- Researchers
 - Verifying trust in used software/hardware
 - To find vulnerabilities





"How?"

- Firstly, Blood, sweat, tears ... and stress. Lets not forget stress.
- Secondly, the toolset used can be classified as..
- Static (this means checking the binary without it running)
 - Hex Editors viewing the hex
 - Debuggers try to move hex to assembly
 - Disassemblers try to move hex to high level code
- Dynamic (fiddling with the binary while it is running)
 - Debuggers can run the binary instruction by instruction
 - Emulators can run binary in a fully contained and controlled setup
- Lastly pen, paper and detective work



n i \mathbf{a} m a

m \mathbf{a} u

"Past Examples"

- 1992 Atari vs. Nintendo
 - Atari RE'ed the machine instructions for Nintendo console so that could produce games for it
 - Atari won
- 1992 Sega vs. Accolade
 - Accolade RE'ed the Sega console so they could produce cartridges
 - Accolade won
- 2001 US vs. Elcomsoft vs. Sklyarov
 - Dimitry gave a DEFCON talk
 - Talk was on cracking the Adobe ebook reader encryption
 - The next day he was arrested
 - Dec 16 2002, Elcomsoft and Dimitry were acquitted

n n i \mathbf{a} m a m a



"Practical"

- Some basic examples, we will use typical game controls ...
- CD check
 - *<practical>*
- Keyfile check
 - \bullet ractical>
- Serial check
 - \bullet ractical>

 \mathbf{n} \mathbf{v} \mathbf{n} i a m a m a u m



"So what does this mean?"

- Be aware
- Do not hide bad code in compiled code
- It is possible to "recover" legacy code
- Use encryption take a page from virus writers
- Learn

n a m a m a



Thank you for your attention

Ollydg - http://www.ollydbg.de/

XVI - http://www.chmaas.handshake.de/delphi/freeware/xvi32/xvi32.htm

Intel Opcodes - http://www.jegerlehner.ch/intel/opcode.html

Conversion table - http://www.laynetworks.com/ASCII%20to%20hex%20value%20chart.htm

Laerning - http://acrigs.com/FRAVIA/FRAVIA index.htm

Crackmes - http://www.crackmes.de/archive/

