Ecole d'ingénieurs et d'architectes de Fribourg
Hochschule für Technik und Architektur Freiburg

Microprocessors 3

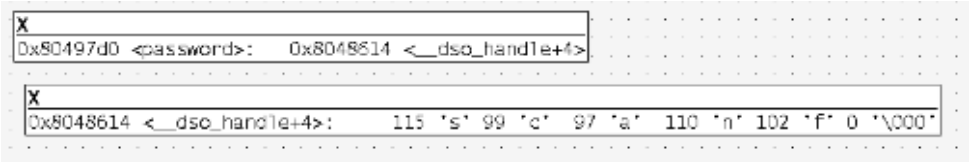
Report lab 4 : Intel Assembler

Jonathan Stoppani et Elias Medawar

Version: March 24, 2011

1 Find the password used by the programm

1. Run the program and analyse the basic functionality
   The program display Enter password
   We enter the password
   The program write Bad password.
2. use the command strings to analyse if there is some relevant string that can be a password.
   To many strings we can not exploit this method
3. objdump -d password_1
   find main section, found a call for strcomp (string compare)
   Just before the call of strcomp will move on the stack 2 arg .
   One arg is the entered password and the second arg is a pointer(0x080497d0).
4. use ddd to find the value of the pointer (display 0x080497d0)
   we found the value 0x08048614
5. use ddd to display the value at address 0x08048614
   we found the password : scanf



1.1 Alternative

1. use readelf -x <24(data)> to read the fixed values
   we found the pointer to the value in the rodata section
2. use readelf -x <15(rodata)> to read the value of the password.
   we found the password: scanf

2 When the password is found, delete the symbols with the command strip and use ddd without symbols

1. strip password_1
2. open the program with ddd
3. with the console add a breakpoint in the main section(break @)
4. with the console run the program and display the values of the pointer