Surreptitious Software

Exercise

Attacks
Decompilation

Christian Collberg
Department of Computer Science, University of Arizona
February 26, 2014

Crack — Discover major algorithms

Have a look at the file `player-decompiled.c` provided to you. It's the output of a decompiler (called `REC`). Examine the code carefully. The original program contains all the different protection methods we discussed in the previous exercises.

1. Can you find them all in the decompiled code?
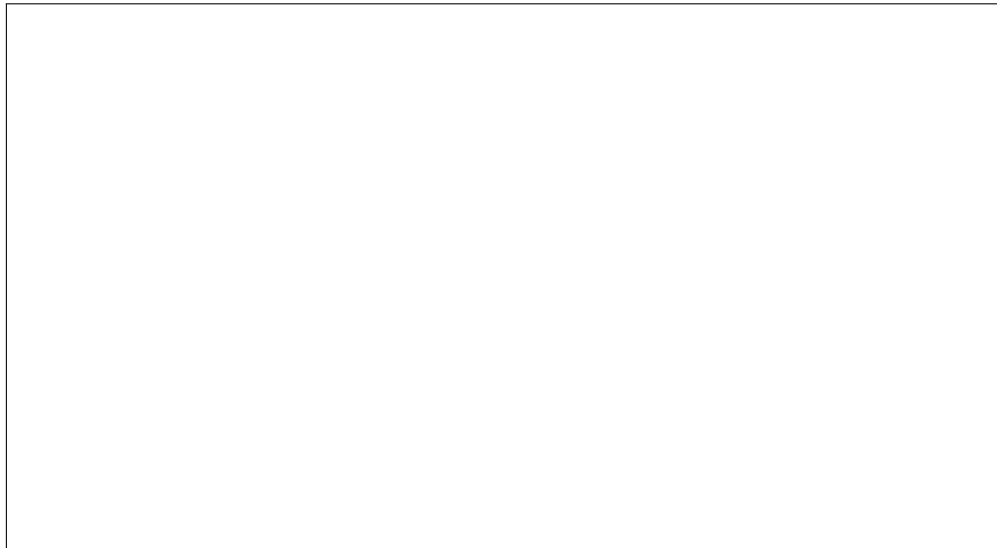
2. What can you learn about the "decryption" function?
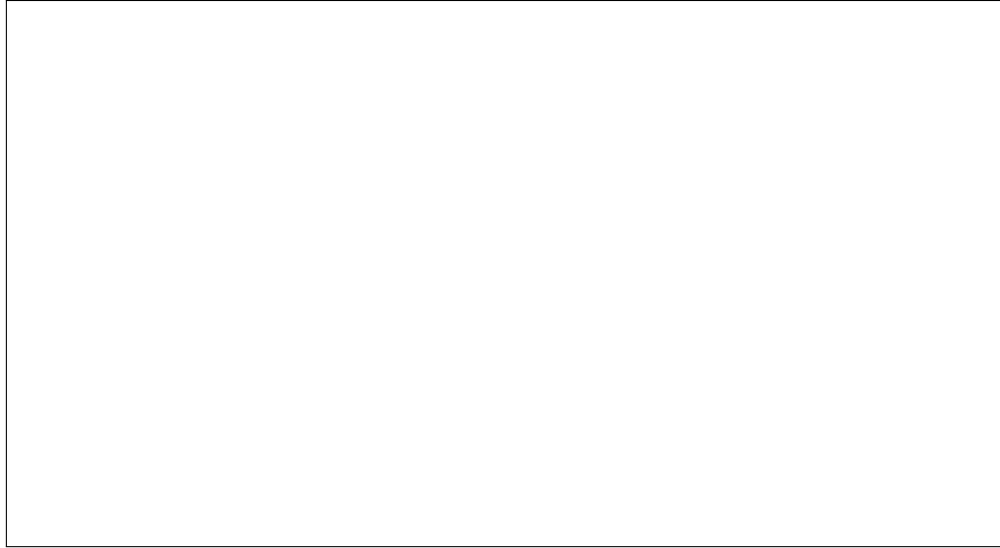
Prerequisites

Before working the exercise make sure you download, install, and build the following:

1. Install the following tools:

tool	url	Linux	MacOS X	Windows
gcc		⚙ gcc build-essential		
REC	www.backerstreet.com/rec/ rec.htm		N/A	N/A

2. Download program and data files:

   (a) `wget 'http://www.cs.arizona.edu/~collberg/tmp/ssx.zip'`
   (b) `unzip ssx.zip`
   (c) `cd ssx/attack-defense_attack4`

3. Install the following tools:

4. Build the `player2` executable which you will be working on from now on:

   ```
   > make
   ```