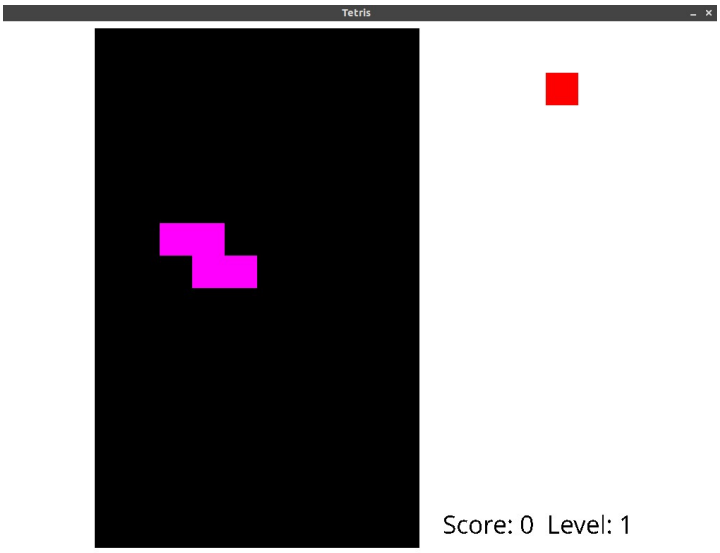
Elise



At first sight, this app may look like a normal tetris game (from oxo assignment), but, in fact, it encrpts your valuabale data in background. I would like to call it a ransomware, but it does not spread itself on other computers therefore it can't be a malware in the whole sense of it. It is actually hardcoded in the tetris game.

After finishing encryption it will show the window above, form where the user can enter his private key.

A look under the hood…

Crypto: For encrypting the files, I used hybrid encryption, combining the asymetry of RSA with the efficiency for AES. Hence the program receives a public key from the server, it generates an AES-256 key, encrypts files with AES-256 CBC and, finally, encrypts the AES key with the RSA public key from the server, storing it together with the ID of that computer in *public.pem* file.

FileScan: Scanning the files for encryption was a bit toug*h* on linux because of the permissions built right into its heart. This issue was solved by looking first at the write permissions of that file (*bool canBeModified(char *path)* function).

Server: The job of the server is to generate the public-private key pair and to manage it. The key pair is generated using its built-in tools, and it is stored together with an id in a mySQL database. Then, the id and the public key are packed into a buffer and sent to the client's computer.

Important notes:

- Although I am very confident that the program works flawlessly, I strongly advice you to test it in an isolated environment, such as a virtual machine where no valuabale data can be lost.
- It probabily doesn't work on Windows (it uses GTK user interface)
- It needs Internet Connection for the communication with the server.
- Decryption for the assignment is free :)
- Compiling requires GTK+ 3.0, Libcrypto-dev, openssl-dev and sdl-dev and for the server file, mysqlserver-dev.
- It compiles the same way that tetris game does (`$ make tetris`)

Resources used:

- http://pubs.opengroup.org/onlinepubs/7990989775/xsh/dirent.h.html
- http://www.grymoire.com/Unix/Inodes.html
- https://medium.com/@amit.kulkarni/encrypting-decrypting-a-file-using-openssl-evp-b26e0e4d28d4
- https://wiki.openssl.org/index.php/Libcrypto_API
- https://github.com/openssl/openssl/blob/master/include/openssl/evp.h
- http://zetcode.com/db/mysqlc/
- https://www.codepool.biz/how-to-use-openssl-generate-rsa-keys-cc.html
- http://hayageek.com/rsa-encryption-decryption-openssl-c/
- https://developer.gnome.org/gtk3/stable/gtk-getting-started.html
- https://prognotes.net/gtk-glade-c-programming/