Hiding and communicate data using games : experimentation using Minecraft

Sébastien Bequignon
(sb788@kent.ac.uk / sebeq33@gmail.com)

MOJANG

- Minecraft is a game based on self-development and 3D environment creation using blocks.
- The game include exploration, gathering resources, crafting, and combat.
- Available on multiple platform using different version (PC/Linux/Mac, Xbox, Smartphones)
- Running using Java Platform
- So far, 14 500 000 peoples on the Computer version of the game.
- Updates of the game each 3 month on average.

The Project

- Creation of an open source software able to hide and communicate valuable information within seemingly harmless content.
- Two different parts :
  - Hide data on the save of the game (Steganography), being able to send the results and decrypt them once at the destination
  - Communicate datas on a real server of the game using a custom client of it.
- Usable on Windows, Linux and OSX

  The server of the game is freely accessible by anyone on the game website.

Open Source Repository : https://github.com/sebeq33/StegoMinecraft

Steganography

- Steganography is the art or practice of concealing a message, image, or file within another message, image, or file.
- In this project :
  - Hide information replacing blocks by binary values

    Block A = 0 / Block B = 1 so ABA give 010
  - Each modified save are playable by common users without expecting data modification

    Use of unbreakable blocks (called Bedrock)
  - Hide data at various places, randomly inserted (with key) or as a box.

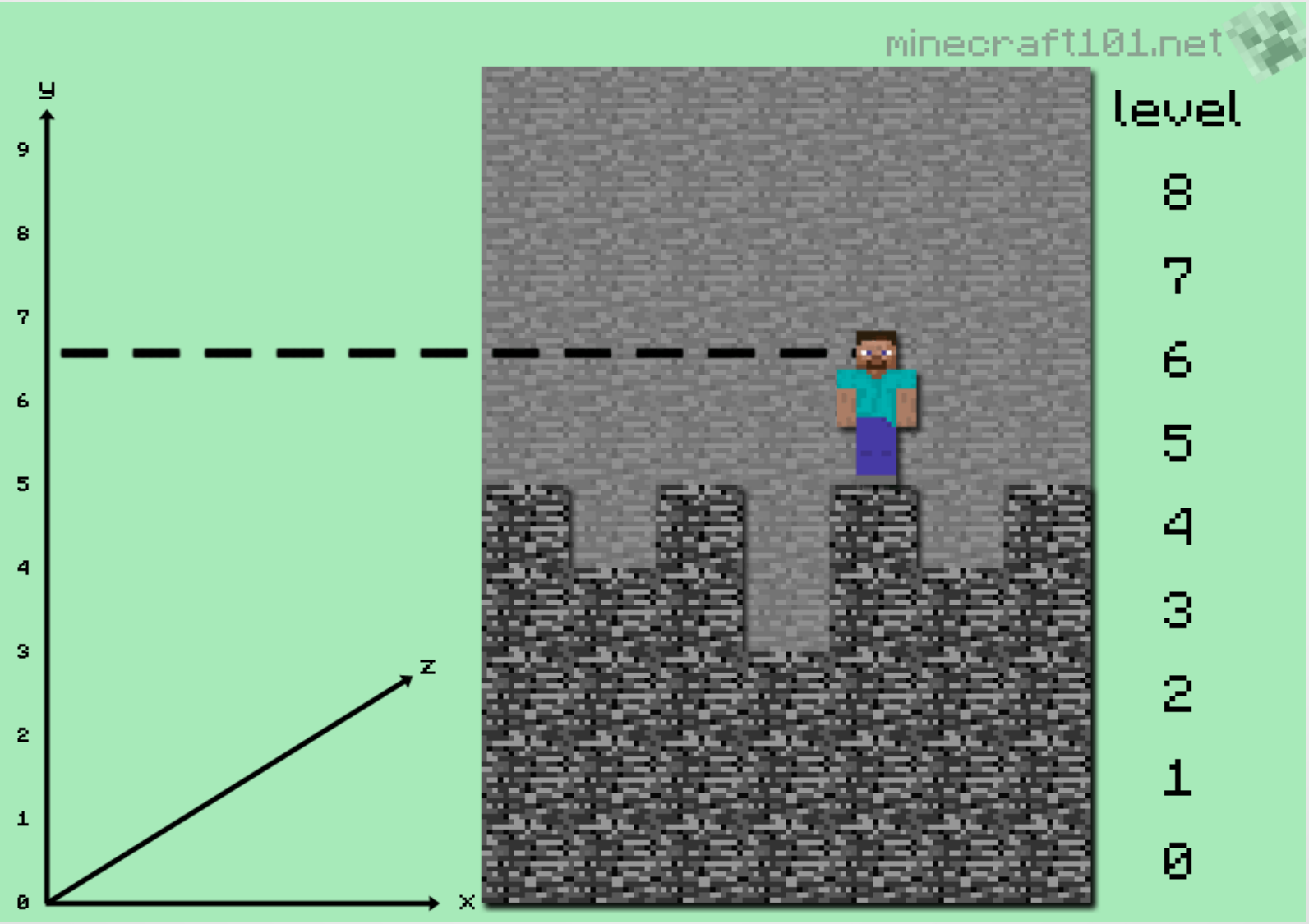
    The position of the data only known by his own creator

Data content

- One save played by a usual player is composed of 50 000 Chunks of blocks.
- A Chunk is a zone of 16 * 16 * 16 (x/y/z) blocks.
- Those are generated while the environment is explored, with the player movements.
- Using only the lower layers (5 * 16 * 16) composing the environment of a save, there is still 1280 blocks free to modify.
- Supposing i store only 1 bit of data by block, i can store 1280 bit of data by chunks.

Ref : http://minecraft.gamepedia.com/Chunk_format

Example



Useful notes

- Each map or level is peuso-randomly generated using a key saved in it.
- If the same key is used to create a map, the exact same map will be created without the modifications of the player or ours.
- We can change the key, but the modification will be obvious.
- If someone use the original key and do the comparison between our map and the copy created, he can find each modified blocks.

  But he can't determine the right order.
- Public maps can be downloaded from the web, these will have lots of initial modifications and could be a lot bigger.
- A played map, where one or plural peoples create content each day, will be also a good material.

Communication

- The purpose is to be able to communicate on a distant server and leave a message accessible by another computer with the software.
- Compression and encryption algorithms can be used to reduce the size of data sent and add a layer of security on the transmission. This part may not be done depending on project advancement, contribution can be made as it is an open source project.
- The communication is done using the protocol already existing on the game, connecting a false player.

Ref : http://www.minecraftforge.net/wiki/Packet_Handling

Protocol

- Use the console's commands as administrator to modify the map and check modifications
- Packet ID : 0x02Field : JSON Data

  Field type : String (varint with length then byte[ ] Limited to 32767 bytes)
- Two useful ingame commands :

  - /testforblock <x> <y> <z> <tilename> [datavalue] [dataTag]

  - /setblock <x> <y> <z> <tilename> [datavalue] [oldblockHandling] [dataTag]

- *Protocol Ref :*
  - *http://wiki.vg/Protocol*
  - *http://minecraft.gamepedia.com/Commands*

- *Varint : Smaller numbers take a smaller number of bytes.*

Language and ressources

- The software use Python 2.7 as programming language
- I am using a programming tool called « pymclevel » for save modifications, for the steganography part of the project.
- The version of the game used Minecraft 1.7.5 (26/02/2014)
- Only use PC / Linux / Mac version based on the same source code.

Purposes and intent

- Propose a useful and appropriate tools when suitable solution or encryption not available.
- Prove that it is relevant to use video games as a means of secure communications
- Use a completly harmless game to secure communication.
- Be able to use a server running since long time ago.
- Being hidden behind 14 000 000 of users growing each days.

- Project inspired by this paper :

  « Steganography in games : A general methodology and its application to the game of Go » (2006)

- Project repository online :

  https://github.com/sebeq33/StegoMinecraft

- My emails :

  - sb788@kent.ac.uk

  - sebeq33@gmail.com

Thanks, Questions ?

Supervisor : Dr Julio Hernandez-Castro (jch27)