User security

1. User authentication

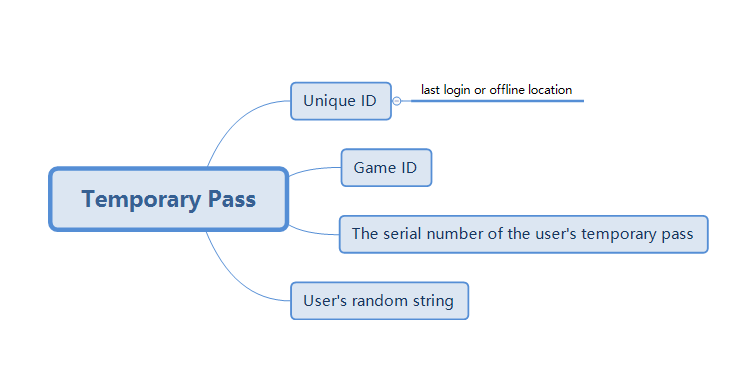
Solution：

1. The user logs in to the server through the https protocol.
2. Start a browser when the user logs in, and when using the https protocol to connect to the server, we encrypt the user's password with MD5 and then pass it to the server for verification and register a temporary pass on the server
3. The server returns the session key and the user's temporary pass. The composition of the session key needs to include the user's IP address and login time. The temporary pass composition needs to include the user's unique ID (last login or offline location), game ID, and user temporary pass. Serial number, user's random string.
4. Use DES encryption
5. After using des to encrypt the temporary pass, save the encrypted password in the server, it is no need to send it to the user.
6. When starting the game, the browser should be closed after the game client is completely sure that it has entered the game, otherwise there may be the possibility of the session key being intercepted, and if so, a warning message will be issued to the user. The temporary pass obtained by the user can ensure that the browser that the user sees is from the official server and not from the Trojan horse website.
7. Finally, the user logs in the game with the temporary pass, and records the unique ID if logging out, and generates a new orderly temporary pass serial number when logging in next time. People who don't know the key can only see a string of meaningless strings each time, and the temporary pass is a one-time use and cannot be forged.

解决方案：用户通过https协议登录服务器。在用户登录时启动一个浏览器，使用https协议连接服务器的时候我们将用户的密码MD5加密以后传到服务器验证并在服务器注册一个临时通行证。服务器返回session key 和用户的临时通行证，其中session key的组成需要包含用户的IP地址和登录时间，临时通行证组成需要包含用户的 unique ID（最后登录或者下线的位置）、游戏ID、用户临时通行证的序号、用户的随机字符串，最后需要des加密。临时通行证des加密后，加密的密码保存在服务器中，不需要传送给用户。在启动游戏时，浏览器应该在游戏client完全确定自己进入游戏后再关闭，否则有可能存在session key被截取的可能性，如果存在则向用户发出警告信息。用户获得的临时通行证可以确保用户看到的浏览器是官方服务器的而不是木马网站的。最后，用户将拿到的临时通行证登录游戏，若登出则记录unique ID，在下一次登录时生成新的有序的临时通行证序号。不知道密钥的人每次只能看到一串无意义的字符串，而且临时通行证是一次性的，都无法被人伪造。



上面是用户认证过程



上面是临时通行证生成方式