# 单机防破解思路和探索

——————戏曹传防破解介绍

# 感谢

- 感谢徐纪昊和张涛杰的贡献

# 防破解内外兼修

- 客户端重点数据（元宝）防护
- 服务器端重点数据（元宝）防护
- 打心理战

# 客户端防护策略

- 安装包代码需要混淆
- 安装包加固
- 客户端内存防护
- 客户端本地数据防护
- 客户端通信防护
- 客户端逻辑和数据自检
- 客户端地雷埋设
- 关键流程需联网执行

# 客户端防护策略

- 代码混淆：代码混淆能够避免破解人员通过简单的反编译或者解压，就能看到游戏客户端的部分代码（特别是java部分）
- 代码加固：利用第三方代码加固加壳，加大破解人员对游戏包体的破解成本。
- 当破解人员的破解成本高于实际获得价值时，则可能会放弃破解。

# 客户端防护策略

- 内存防护：针对内存中的缓存值进行防护。同人单机战棋游戏，在游戏过程中，会将大量的数据保存在内存中，用于游戏过程中的读取或者计算，当结算后，再保存于本地文件中。在内存中保留数据时，直接以数值的形式保存各关键数据。破解玩家利用内存修改器，利用同一个物品改变数量时，内存地址不变的特性，进行内存地址的锁定，当锁定到后，利用工具进行修改。为了避免原有逻辑不变和修改的影响域最小，戏曹在关键数据“元宝”存储上，进行数值的替换，即在内存中存元宝值时，使用数据字典映射的方式存储，在游戏启动时，内存中构建一张0-9对应的英文字母字典，元宝数值要存取时，利用字典变换，实际内存中存储的是英文字母。以避免利用内存修改器进行初级的搜索。

# 客户端防护策略

- 本地数据防护：单机游戏，玩家的购买记录、关卡锁，元宝数量都是记录在一个payrecord文件中。破解玩家时常利用替换payrecord文件的方式获取破解的内容。戏曹在该方面的防护策略是使用md5码进行加密校验。加密时，利用密钥，玩家token，玩家payrecord文件内容作为加密内容进行md5码的生成，存储在本地另一个文件中，若玩家只替换payrecord文件，则校验生成的结果和所存md5码不同。校验失败后，则客户端可以进行主动的闪退。

# 客户端防护策略

- 通信防护：在与服务器端通信时，对一些重要的通信进行加密，两边在收取对方信息时，可以进行通信传递的内容的md5码校验，以确保在传递过程中信息没有被修改。

# 客户端防护策略

- 逻辑和数据自检：破解玩家进行破解时，由于未完成正常的流程，所以玩家数据在某些逻辑上产生了不连贯，不一致性。比如，玩家通过内存修改方式修改出武将或者物品时，则在该玩家的购买记录里不会存在该物品的购买记录。针对一些内购物品或者后期新出物品，可以利用物品列表与购买列表的检查来判断玩家是否进行破解，若发现，客户端进行闪退。

# 客户端防护策略

- 地雷策略：该策略的想法思路较主动，即在一些重要数据或者流程中，埋设陷阱，一旦玩家触发，则进行闪退引爆客户端。例如，在客户端内存中埋设多份与元宝值一致的数据值，一旦玩家修改这些值，则进行引爆。

# 客户端防护策略

- 重要流程联网执行：在一些重要流程中，必须执行联网，确保针对操作数据的校验和服务器数据的同步更新。例如，玩家进行商城购买时，必须进行联网，服务器端针对玩家的操作数据进行校验，若发现异常，则不让其进行购买流程，客户端本地也不进行记录。

# 服务器端防护策略

- 客户端数据不信任策略
- 玩家数据采集
- 客户端数据校验
- 主动通知策略
- 关键流程的服务器化

# 服务器端防护策略

- 客户端数据不信任策略：服务器端不能无条件的信任从客户端发送过来的数据。对于重点数据，必须只信任服务器端，例如单机游戏中的元宝，该值只能在服务器端进行数值操作，客户端进行接受和显示。而对于网游端，则需要关注更多的数值。

# 服务器端防护策略

- 玩家数据采集：玩家数据能反应玩家在整个游戏过程中的游戏行为，需要对玩家的一些重点数据进行采集，以此可以分析玩家的游戏情况，进行诊断，不能因为玩家是以游客身份进行游戏，而对其不做数据采集。例如：戏曹传中对游客玩家的数据进行采集，游客玩家也在服务器上存有一份对应的payrecord信息和充值信息，用于反破解的处理。

# 服务器端防护策略

- 客户端数据校验：基于玩家数据不信任策略，利用已采集的玩家数据，我们可以针对玩家客户端上传上来的数据进行校验。若经过一系列的判断，发现玩家的数据异常，则服务器不进行接受存储该数据，以及对关键的异常数据进行记录，以便日后追踪。

# 服务器端防护策略

- 主动通知策略：客户端与服务器可以约定协议命令，一旦客户端收到该协议命令则进行客户端的主动闪退，配合客户端在关键流程上必须联网，进行一系列的数据检查，服务器则能通知客户端是否闪退。

# 服务器端防护策略

- 关键流程的服务器化：对于一些通用的，关键性的流程（对于单机部分来说可以认为是充值和元宝商城内购）除了上述策略作防护之外，其实可以有条件的进行服务器化的处理，例如，可以将内购的部分关键流程作到服务器上，例如客户端通知服务器端，我要购买某样物品，服务器端进行对玩家的元宝扣除和对已购商品列表的维护。

# 打心理战

- 打心理战：防破解是一个竞争，和破解玩家的竞争，玩家的破解手法可以是多种多样的，但是95%的购买破解的玩家有一个根本的诉求：近乎免费的玩到同人游戏。当他付出的代价超出他的近乎免费的标准，并且，破解游戏进行体验时，会冒着各种闪退和封号的风险时，他们则会考虑是否需要破解。

- 而剩余那部分主动研究破解，希望通过破解谋利的人，我们则通过越来越严苛的防破解措施，让他放弃破解，若他觉得破解是一个很麻烦的事情，也许他会考虑放弃破解。


# 经验分享完毕

谢谢