广西科学院学报
Journal of Guangxi Academy of Sciences

2010,26(1):35～37
Vol. 26,No. 1 February 2010

实施软件保护反外挂技术的一款网络游戏开发
The Implementation of an Anti Illegal-Plug-Game Technology Based on Software Protection

高 翊
GAO Yi

(南宁市平方软件新技术有限责任公司,广西南宁 530003)
(Nanning Pingsoft New Technology Co. ,Ltd. ,Nanning,Guangxi,530003,China)

摘要:描述实施软件保护反外挂技术网络游戏的开发环境、运营环境和具体实施情况,然后对实施反外挂技术的网络游戏进行模拟与控制式外挂和监听与修改式外挂攻击测试,验证基于软件保护的反外挂技术的可行性和正确性。

关键词:游戏 反外挂 软件 保护 可行性 正确性
中图法分类号:TP311.52 **文献标识码**:A **文章编号**:1002-7378(2010)01-0035-03

Abstract: The implementing and testing of an anti illegal-plug-game technology on a MMORPG web game is illustrated. According to the analysis of the anti illegal-plug-game technology effects and the game performancing before and after the implementation, the feasibility and correctness of the deep solution for the anti illegal-plug game is validated.

Key words: game, anti illegal-plug, software, safeguard, feasibility, correctness

实施软件保护反外挂技术的以西方文化为背景的奇幻 MMORPG 网络游戏,是一个架构在幻想世界中发生的故事,有人类、恶魔、狼人等不同的种族和部落,以及各色各样的邪恶角色与魔物,玩家可以在这个虚拟世界中赋予角色多种不同的职业,战士、牧师、魔法师、工匠等,满足各种角色参与的体验。游戏没有固定的剧情束缚而有丰富的任务系统,使得游戏变幻莫测。游戏具有强大的 3D 图形渲染功能,使用了基于 OpenGL 的图形显示技术,拥有绚丽柔和的室内外场景,夺目的魔法效果,精致的以及流畅的人物动作系统。游戏的网络架构多元化,让游戏世界可以随时进行扩展,任意改变地图。无论从游戏内容、风格上,还是从游戏开发技术和运营模式上看,这款游戏都是现今很具有代表性的一款 MMORPG 游戏,在该游戏中实施深度保护反外挂技术[1],具有很高的普遍性和实用性,研究成果值得其他网络游戏予以借鉴。

收稿日期:2009-10-29

作者简介:高 翊(1974-),男,硕士,主要从事网络游戏开发和软件保护方面的研究工作。

1 游戏的开发环境

该款游戏的客户端和服务器端的开发平台都是 Windows,开发语言为 C++,开发和编译环境是 Visual. NET。用户帐号数据库和游戏资料数据库采用的都是微软的 SQL SERVER。帐号校验和收费系统、用户登陆系统是基于 JAVA 开发的,与数据库的接口为 JDBC。

2 游戏的运营环境

游戏的正常运行需要后台服务器组(图 1)的支持。后台服务器组主要包括客户端资料更新服务器、用户帐号数据库、帐号校验和收费服务器、服务器组选择服务器游戏资料数据库、游戏资料存储服务器、转发服务器和多台游戏服务器。后台游戏服务器组中的服务器都是运行在 Windows 操作系统下。

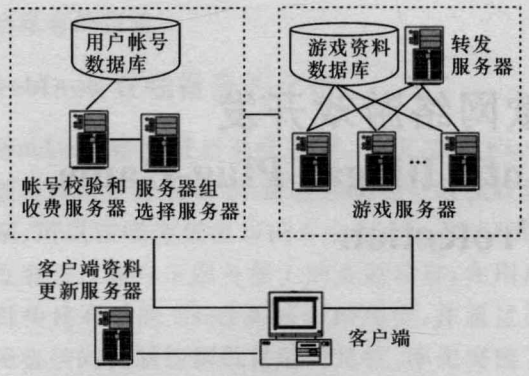

图1 游戏服务器组的系统架构

3 游戏的软件保护反外挂技术实施

在游戏还处于开发阶段、没有进入正式商业运行时，将基于软件保护的反外挂技术代码作为游戏的功能模块加入到游戏代码中。通过加密、反编译和反调试等手段，使黑客无法得到代码，通过反篡改等技术保护程序不被外部程序修改，达到防止监听与修改式外挂软件的目的，抵制了模拟与控制式外挂的入侵。

4 游戏的效果验证

游戏的效果测试主要包括两大部分。第一部分是与之前没有采用基于软件保护反外挂技术的网络游戏之间进行比较，从各个角度测试反外挂的效果，包括对模拟/控制式外挂和监听/修改式外挂两类外挂的防止效果比较；第二部分是测试使用反外挂技术后的网络游戏原有性能是否受到影响。

4.1 测试环境

服务器硬件配置和运行环境为：HP DL380，CPU Xeon 至强 2.8G，内存 1G，硬盘 40G，操作系统为 Windows2000 Server，数据库为 SQL Server 2000。

客户端硬件配置和运行环境为：CPU Intel 2.4G，内存 512M，硬盘 80G，操作系统为 Windows2000 Server。

4.2 针对模拟与控制式外挂的反外挂效果验证

测试内容：使用键盘精灵、鼠标精灵等模拟键盘、鼠标工具，设置好键盘和鼠标的操作，对客户端程序进行攻击。

测试结果：未使用反外挂技术的程序，可以不使用键盘和鼠标进行游戏，根据事先设计好的键盘、鼠标控制进行操作。使用反外挂技术后程序能够检测到鼠标和键盘的侵入异常错误，并退出程序。

4.3 针对监听与修改式外挂的反外挂效果验证

4.3.1 使用代码加密的测试比较

测试内容：使用 W32Dasm 静态分析工具对网络游戏客户端程序进行反编译，得到汇编代码，找到网络通讯协议部分和键盘、鼠标接口部分的代码。

测试结果：未使用反外挂技术的程序机器码被反编译出来(图 2)，使用反外挂技术后得到的汇编语言是乱码，无法从中得到有用的信息(图 3)。

图2 未使用加密技术被反编译结果

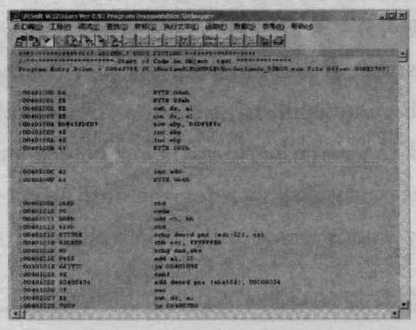

图3 经过加密后反编译的结果

4.3.2 使用反破解技术的测试比较

测试内容：依然使用 W32Dasm 的静态分析工具对客户端程序进行反编译，得到代码。

测试结果：未使用反外挂技术的程序机器码被反编译出来(图 3)，使用反外挂技术后的程序，尽管可以反汇编并得到汇编语言，但是得到的代码与原来的代码已经完全不同(图 4)，黑客无法知道程序的结构。

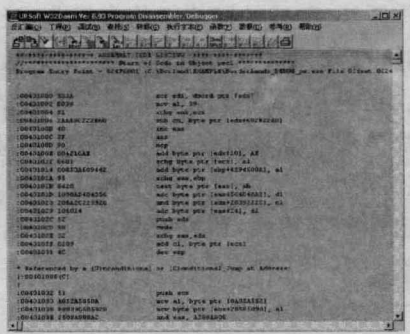

图4 经过代码反破解(迷惑)后反编译的结果

4.3.3 使用调试监视技术的测试比较

测试内容：使用 OLLYDBG 的动态调试器对客

户端程序进行调试。

测试结果:未使用反外挂技术的程序被OLLYDBG工具跟踪调试,并能够正常进入游戏。使用反外挂技术后的程序被OLLYDBG跟踪后,OLLYDBG调试器停在INT 1语句处(图5),而无法正常进入游戏。

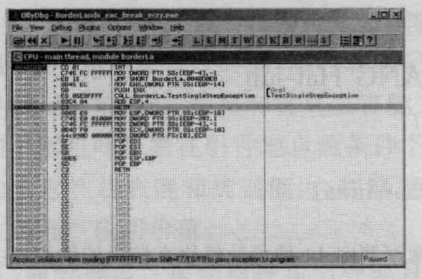

图5　程序检查到有调试器时产生异常的调试器停住

4.3.4　使用反调试技术的测试比较

测试内容:依然使用OLLYDBG的动态调试器对客户端程序进行调试,在程序中设置断点,并查看寄存器。

测试结果:未使用反外挂技术的程序被OLLYDBG工具跟踪调试,并可以在程序中打断点,观察到程序的执行情况以及寄存器、变量的变化。使用反外挂技术后的程序被OLLYDBG跟踪后,OLLYDBG停顿在异常处理的代码(图6),而无法进入游戏。

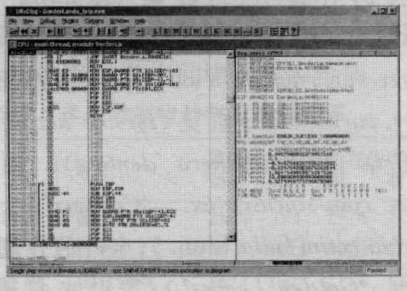

图6　程序发现有断点时产生异常的调试器停住

4.4　使用反外挂技术前后的性能比较

4.4.1　可用性测试

可用性指的是需要访问信息的用户可以在不受干涉和阻碍的情况下对信息进行访问并按所需格式接收[2]。测试内容为正常登陆游戏后,让客户端与服务器和其他客户端交互,完成游戏中的交互性功能。测试结果是用户评价的两个客户端程序完成的功能一样,用户体验效果一样。

4.4.2　精确性测试

精确性是信息免于出错并具有终端用户期望的结果[2]。测试内容为正常登陆游戏后,对游戏中客户端每个功能进行测试,如界面的操作。测试结果是两个客户端程序能够完成的所有功能一致。

4.4.3　完整性

完整性是指保持完整而质量和状态未被破坏[2]。测试内容是正常登陆游戏后,对游戏的显示速度进行测试;选定进入恶魔地图的某一固定场景进行测试,比较前后的结果。测试结果是每帧显示画面的FPS(Frame Per Second 每秒显示帧数)测试,未使用反外挂技术的程序为28.2FPS,使用反外挂技术的程序为27.4FPS。

4.5　测试结果比较

采用基于代码安全的软件保护反外挂技术后的网络游戏反外挂能力明显加强,很好的防止了多种黑客工具的攻击,对模拟与控制式外挂和监听与修改式外挂两类外挂都能起到防护的作用。而且使用反外挂技术后对游戏完整性、可用性等性能没有太大影响,保证了游戏的正常运行。所以基于代码安全的软件保护反外挂技术可以正确防止模拟与控制式外挂和监听与修改式外挂两类外挂攻击。

5　结束语

基于软件保护的反外挂技术实施于网络游戏中,对模拟与控制式外挂和监听与修改式外挂两类外挂攻击都能起到防护的作用,而且使用反外挂技术对游戏的完整性、可用性等性能没有太大影响。但是作为一种新的反外挂技术,还需要在更多实践中加以校验和完善。本文测试方案针对的是两类外挂,同时兼顾防止黑客制作部分外挂的能力。但是,网络游戏与其他软件行业的产品很类似,如果游戏软件反外挂能力越强,那它的目标就会越大,因为对于外挂制作者来说,更值得去尝试,更有兴趣来破解,可能从而产生新功能的外挂,所谓魔高一尺,道高一丈。所以本文的研究和试验只能是阶段性成果,还需要继续对今后出现的新型网络游戏外挂做紧密的跟踪研究,不断提高反外挂技术水平和能力,有效地保护正规网络游戏的正常运营,保证开发商、运营商、合法用户的利益,促进中国游戏产业的发展。

参考文献:

[1]　高翊,张旸旸.游戏反外挂技术方案的设计和实现方法[J].广西科学院学报,2009,25(4):327-329,332.

[2]　Michael E Whitman,Herbert J Mattord.信息安全原理[M].徐焱,译.北京:清华大学出版社,2004.

(责任编辑:邓大玉)