<<网络游戏安全揭密>>

图书基本信息

书名：<<网络游戏安全揭密>>

13位ISBN编号：9787111255222

10位ISBN编号：7111255224

出版时间：2009-2

出版时间：机械工业出版社

作者：Greg Hoglund,Gary McGraw

页数：219

译者：姚晓光

前言

入侵游戏的诱惑　　如果有一天，突然有人对你说“你要交200元的罚款才可以离开”，千万不要以为你是因违犯交通规则而被交警抓了，而是因为你在网游中使用“外挂”，被游戏程序自动“抓捕”了，要交200元的罚款。

如果有机会，很多人会作弊，尤其是认为自己不会被抓到的时候。

网络上可以很容易匿名，这就让作弊更具吸引力。

游戏是软件，是软件就有缺陷，这是来自人类开发者的DNA。

每天都有很多人使用网络游戏的外挂和辅助工具，其中部分玩家是因为太忙，虽然很想玩但没有办法投入太多时间，不得不采用作弊的方式。

为了改变网络游戏岌岌可危的安全局势，游戏开发人员必须在软件安全方面做得更好，毕竟任何公司都没有权利通过对玩家罚款来制止外挂。

提高网络游戏安全性的第一步，就是掌握游戏被入侵时实际发生的情况。

那么　　游戏是如何被入侵的呢？

我们又该如何防范呢？

有哪些方法可以找到软件的漏洞呢？

这就是本书所要说的。

书中以《魔兽世界》等MMO-RPG游戏为典型案例进行分析，非常清楚完整地展示了人侵的代码，从简单的宏指令到复杂的系统后门入侵方法，都毫不保留地展示。

在本书中网络游戏就像是软件安全方面一个相当有趣的实验品。

网游的安全问题阻碍游戏的成功　　随着竞争越来越激烈，游戏研发、代理、运维、营销的成本越来越高，信息和电子对抗本来就是一场精彩的较量，网络游戏的设计有着很多缺陷，例如：“两种技能的叠加”就是一种找漏洞的策略。

在《魔兽世界》中魔法交互作用的结果会很惊人。

在有的宠物身上使用“豹群守护”魔法，然后让它攻击远处的怪物，紧接着在“飞行点”搭乘飞行坐骑。

通过这两种技能的组合，有趣的状态发生了。

在这个例子中，你并没有开始自动飞行，而是获得了飞行坐骑的控制权，可以自己驾驶坐鹰了。

这类问题并不限于《魔兽世界》，状态组合攻击对大部分的MMO-RpG都有效，利用状态时间差甚至可以复制网络游戏中的装备和金钱。

当然除了找到游戏设计缺陷，本书的精华部分更在于第6、7、8章所介绍的入侵技术和手段。

其中谈到的破解技术：自动控制键盘鼠标、像素采样、数据包传递和截获、覆盖率测试工具、反编译、反汇编、故障注入引擎、逆向代码工程、动态跟踪、注入DLL文件、内存伪造等技术。

这些内容不管是针对游戏，还是其他软件都非常重要。

这些技术的掌握程度是区分初级破解者和资深破解人员的标志。

<<网络游戏安全揭密>>

内容概要

《网络游戏安全揭密》主要介绍了游戏被入侵的机理、防范手段及找到软件漏洞的方法。《网络游戏安全揭密》以《魔兽世界》等MMO.RPG游戏为典型案例进行分析，非常清楚完整地展示了入侵代码，从简单的宏指令到复杂的系统后门入侵方法，都毫不保留地进行了展示。《网络游戏安全揭密》中的网络游戏就像是软件安全方面一个相当有趣的实验品。

《网络游戏安全揭密》适合软件开发、游戏开发人员等阅读。

作者简介

Greg Hoglund，软件安全领域的领军人物，一位依靠自学成才的天才黑客。
他成立了一系列的从事计算机安全方面的公司，其中包括著名Cenzic和BugScan，目前正打理他自己创立的第三家公司——HBGary。
专门致力于如何在黑客正在入侵和破解的时候迅速地捕捉到黑客信息，主要的服务对象是美国国防部。

Gary McGraw全球公认的软件安全权威，Cigital公司的CTO，董事会成员，掌管Fortify软件公司的技术顾问团，同时担任Raven white司的膏级顾问。
Gary在网络安垒方面著有多本著作，其中的6本长居销书排行前列。

译者简介：　　姚晓光，npce.com创始人。
现任腾讯公司游戏项目总监。
曾任盛大网络盛锦游戏公司常务副总经理，游戏首席制作人：监制中国第一款回合MMORPG《幻曼游侠》，监制中国第-款真3D商业网游《神迹》，带领研发《QQ飞车》创50万人同时在线；编译《网络游戏开发》等书被选为游戏研发教材。

<<网络游戏安全揭密>>

书籍目录

关于本书的评论译者序序言前言作译者简介第1章 为什么选择游戏这个主题1.1 全世界的网络游戏1.2 在MMORPG中作弊的诱惑1.2.1 作弊代码1.2.2 犯罪型作弊1.2.3 将虚拟转换为货币：从入侵到道具1.3 游戏也是软件1.3.1 基本游戏结构1.3.2 游戏客户端1.3.3 客户端状态1.3.4 和其他软件类似的功能1.4 入侵游戏1.4.1 谁在入侵网络游戏1.4.2 为什么入侵游戏1.4.3 如何入侵游戏1.4.4 到底有多少起游戏入侵事件1.5 最大的课题：软件的缺陷第2章 游戏黑客的基本方式2.1 网络对抗盗版2.2 另一方面2.3 作弊的诀窍与技巧2.3.1 制作外挂机器人：自动进行游戏2.3.2 利用玩家界面：键盘、点击以及色区2.3.3 使用代理软件：截取数据包2.3.4 操作内存：改写数据2.3.5 利用调试器：断点2.3.6 预测未来：可预知的和随机的如何在在线扑克中作弊2.4 机器人大阅兵2.4.1 自动战斗宏2.4.2 自动瞄准机器人2.4.3 扑克机器人2.5 潜伏(数据虹吸)2.5.1 网络统计2.5.2 扑克统计2.5.3 拍卖操作2.6 正式开工2.7 对策2.7.1 间谍软件2.7.2 典狱官(the Warden，暴雪的反检测机制)：防范过度的反作弊措施2.7.3 总督2.7.4 你的立场在哪里2.7.5 作弊第3章 金钱3.1 游戏公司如何赚钱3.2 虚拟世界：游戏经济学与经济3.2.1 和真实经济体的联系3.2.2 中间人3.2.3 为了赚钱玩游戏3.2.4 Thottbot3.3 犯罪行为第4章 进入律师视野4.1 合法4.2 公平使用和著作权法4.3 数字信息千年著作权法4.4 最终用户许可协议4.4.1 索尼BMG的EULA：大量的rootkit4.4.2 暴雪的EULA：你的内存都属于我们的监视范围4.4.3 Gator的EULA：从不受欢迎的访客4.4.4 微软FrontPage2002的ELILA：友好点，因为你别无选择4.4.5 带有EULA的病毒：病毒软件合法化4.4.6 苹果电脑的EULA：无穷与超越4.4.7 EUIA大阅兵4.4.8 禁止破解4.4.9 禁止游戏入侵4.4.10 财产权4.5 使用条款4.5.1 禁令4.5.2 被起诉不等于违法4.6 盗窃软件与游戏入侵第5章 被程序bug包围5.1 游戏中的时间和状态bug5.1.1 如何免费玩游戏5.1.2 用bug扰乱状态边界5.1.3 使用botnet引发游戏服务器延迟5.1.4 利用bug改变角色状态5.2 游戏中的路线bug5.3 改变用户界面5.4 修改客户端游戏数据5.5 监控掉落物和重生点5.6 只要露个脸就可以5.7 结论第6章 入侵游戏客户端6.1 恶意的软件扫描测试(攻击者的入口)6.2 对逆向工程的防范对策6.2.1 代码打包6.2.2 反调试6.3 数据，数据，无处不在6.3.1 数据曝光的对策6.3.2 动态数据和静态数据6.3.3 在别处寻找数据6.4 在游戏周边得到所有的信息6.5 在游戏软件上层：控制用户界面6.5.1 控制键盘敲击6.5.2 神奇的键盘队列6.5.3 控制鼠标释放6.5.4 像素点颜色采样6.5.5 对付按键精灵的措施6.5.6 产生窗口消息6.6 游戏之内：操纵游戏对象6.6.1 动态内存问题6.6.2 围绕一些被怀疑的对象6.6.3 读取磁盘文件6.6.4 解析可执行文件PE头格式6.6.5 查找游戏对象6.6.6 构建WoW反编译器6.6.7 读写进程内存6.7 游戏之下：操纵表现信息6.7.1 3D=Xy，Z6.7.2 穿墙技术6.7.3 DLL注入6.7.4 隐藏注入DLL文件6.8 游戏之路：操纵网络数据包6.9 最终之路：从内核操纵客户端6.10 结论第7章 “外挂”软件技术点7.1 外挂制作基础7.1.1 事件驱动设计7.1.2 状态机7.1.3 移动玩家角色7.1.4 控制玩家角色战斗7.1.5 自动拾取7.1.6 怪物选择及过滤7.1.7 “引怪”的模式管理7.2 外挂作为调试器7.2.1 调试循环7.2.2 SetProcessKillOnExit7.2.3 SetDebugPriviledge7.2.4 断点7.2.5 从上下文获取信息7.2.6 用断点拉取链接信息7.3 Wowzer外挂引擎7.4 外挂制作高级技巧7.4.1 外挂和内核7.4.2 战斗辅助工具7.4.3 外挂用户界面7.5 外挂制作结论第8章 软件逆向工程8.1 游戏破解8.1.1 代码逆向过程8.1.2 导入和导出函数8.1.3 字符串8.1.4 静态分析8.1.5 动态跟踪8.2 汇编编码模式8.2.1 数据传送操作基础8.2.2 比较操作基础8.2.3 字符串操作8.2.4 函数8.2.5 C++对象8.2.6 异常处理8.2.7 switch语句8.3 自修改代码及“加壳”8.4 逆向工程总结第9章 高级黑客技术9.1 资源替换和改装9.1.1 完全替换9.1.2 重写客户端9.1.3 重写服务端9.1.4 客户端渲染选项9.1.5 模型建构9.1.6 贴图9.1.7 地形9.2 资源文件格式9.3 模拟型服务端(私服)9.3.1 通信协议模仿9.3.2 进入游戏世界必需的几个步骤9.4 法律纠纷第10章 安全是游戏成功的基础10.1 游戏开发中的安全机制建立10.1.1 软件安全Fouch-points10.1.2 黑帽子和白帽子10.2 作为玩家的安全问题10.3 入侵网络游戏

章节摘录

1.3.3客户端状态　　游戏中发生着各种事情，尤其是当成千上万的玩家实时发生互动的时候。
游戏有一个中央服务引擎，接收所有玩家输入，并且随着时间更新游戏世界。
就像所有电脑程序都有一个状态一样，游戏也有一个状态。
系统的状态被定义为一个当前所有内存、所有二级存储、所有寄存器以及系统其他组成部分的集合。
问题是，当前的网络不够快，无法让所有的游戏状态都存放在服务器端，并且同步迅速发送到所有客户端。
为了解决这个问题，也为了让游戏更顺畅地运行，游戏设计师往往允许客户端保存和管理某些“不重要”的状态。
虽然让客户端来保存状态理由很充分，但是任何客户端上的状态都会带来严重的安全风险。
如我们第2章所言，客户端状态是被攻击的首要目标之一。
另一个严重的安全问题跟时间有关。
对分布式系统的一种高级攻击方式是利用状态的临界时间点。
当一个系统是以与服务器通信作为基础的时候，“竞态”（临界状态）条件和其他利用时间点的攻击都很有效。
最常见的一种攻击WoW的方式就是利用服务器例行重启时产生的“竞态”条件。

媒体关注与评论

“这个世界的网络化进程越来越快。
当我还在警惕网上的投票行为时，网络游戏已经暴风骤雨般地铺开了。
新时代到来了，游戏中的虚拟道具也可以具备真实货币的价值，因此财富可以通过这些虚拟物品而累积或消失，这对于玩家来说，构成了一定威胁。
为了知道如何防护这种威胁，你必须理解这些危害是怎么回事。
本书是我见过的最深入最详尽地介绍如何入侵网络游戏的图书，我相信每一个WhiteHat都应该阅读此书。
这可以让你们紧紧跟随着那些黑客们的步伐。
”　　——Avid D.Rubin博士　约翰霍普金斯大学信息安全研究所计算机科学教授
　“所有人都在讨论虚拟世界，但是却没有人去讨论虚拟世界里的安全。
Greg.HoSlund和GaryMcGraw在本书中完美地叙述了目前网络游戏中的安全问题。
”　　———Cade Metz　《PC杂志》资深主编　　“在如何改进安全隐患方面，本书指出了一条正确的道路。
正如本书作者所说的，当你面对着这些可憎的恶魔时，你需要有经验的同伴一起作战，就像持起亚瑟王之剑那样披荆斩棘。
”　　——Edward WFelten博士　普林斯顿大学信息技术中心主任，计算机科学与公共事业教授　　“游戏经常用于现代军事演习来衡量技术进步带来的成果，尤其是空军演习。
本书的讨论方式也类似这一概念，将目标定为“入侵游戏”，来衡量一个游戏的安全性。
对于目前较为严重的计算机系统安全问题来说，本书意义甚广。
”　　“大规模分布式系统将会是未来四分之一个世纪里软件发展的方向。
我们需要去熟悉它们是如何运作的，并且更重要的是理解它们是如何因为安全隐患被入侵的。
本书堪称此学术领域的奠基之作。
”　　——Daniel McGarvey　美国空军信息防护委员会主席　　“就像孩子一样，Gary和我都是通过游戏而深入了解了计算机（而后是计算机安全）。
起初我们沉溺于玩Apple][s上的游戏，但后来发现游戏太少又很贵。
于是我们互相拷贝对方的游戏，但发现这些游戏有版权保护措施，于是我们开始研究如何破解这些保护措施。
但后来发现，破解这些游戏远比玩它们更有乐趣了。
”　　“随着如今网络游戏行业的蓬勃发展，人们不再仅仅是因为兴趣而去入侵游戏，而是为了现实的金钱。
这是无法阻止的一个趋势。
但首先，本书揭示了目前黑客们常用的一些入侵技术。
”　　——GregMorrisett博聿　哈佛大学工程学与应用科学学院计算机科学教授
　“如果你现在是一名网络游戏的玩家但你却不了解网游中的安全，那你的游戏经历是不完整的；如果你正在编写一个大规模分布式软件系统但你又不参考网游，那你就落伍了。
”　　——BrianChess博士　Fortify Software创建者、首席技术师，StaticAnalysis中安全模块的制作者之一　　“这本书以一种全新的视角来看待软件安全问题：去攻击一个网络游戏。
新手一定会觉得本书充满了新奇之感，而老手们也会享受到独特的感觉，比如发现自己以前编程的一些错误，而且只有大规模的多人在线的网络游戏才可以揭示到这一点!太棒了!”
　——Pravir Chandra Cigiml首席顾问OpenSSL网络安全模块的制作者之一

<<网络游戏安全揭密>>

编辑推荐

无论你是玩家，游戏开发者还是软件安全专家，甚至只是对破解感兴趣的爱好者，你都可以在《网络游戏安全揭密》中学习到网络游戏内部的安全机制。

《网络游戏安全揭密》由美国畅销书Exploting software作者和为美国国防部服务的“破解天才”Greg hoglund联袂打造。

《网络游戏安全揭密》为读者真实地展示了诸如《魔兽世界》、《第二人生》等MMORPG中的安全问题，同时，也毫无保留地展示了调试器、机器人、外挂的源代码，来深入浅出地描述网游安全这个主题　　内容包括：　　·为什么说网络游戏的安全是产品成功运营的关键？

·几百万的玩家是如何创造出几十亿的虚拟财富的？

·游戏公司是如何侵犯玩家隐私的？

·为什么玩家要作弊？

·入侵网络游戏有哪些技术手段？

·如何创建一个外挂或者机器人来玩游戏？

·如何替换模型和改造游戏？

《网络游戏安全揭密》由世界著名的软件安全专家所著，详尽介绍了高级大规模分布式软件中的安全问题。

如今的网络游戏通常拥有几百万至几千万的用户，这对软件的未来发展具有指导意义。

《网络游戏安全揭秘》所介绍的黑客攻击和防护技术，也将会是未来软件安全技术问题的重点。

“在足球比赛中，如果只一味防守却不去关注对方的进攻会发生什么情况？

你将无法得知对方什么时候会杀过来，不知道如何去防守对方的传接渗透，也不知道如何发动一次闪电战般的进攻。

在计算机网络领域也是这样，要做好防护工作，必须先清楚如何去进行攻击。

我常常在我的课程里说到，你应该是第一个去攻击自己计算机系统的人，而不是最后一个。

”

版权说明