腾讯游戏安全高级工程师胡和君：定制化对抗——游戏反外挂的安全实践

原创

csdn业界要闻 于 2017-12-01 16:40:00 发布 2139 收藏 10
文章标签： 腾讯游戏 胡和君 看雪安全开发者峰会 安全数据库系统

11月18号，2017看雪安全开发者峰会在北京悠唐皇冠假日酒店举行。来自全国各地的开发人员、网络安全爱好者及相应领域顶尖专家，在2017看雪安全开发者峰会汇聚一堂，只为这场“安全与开发”的技术盛宴。

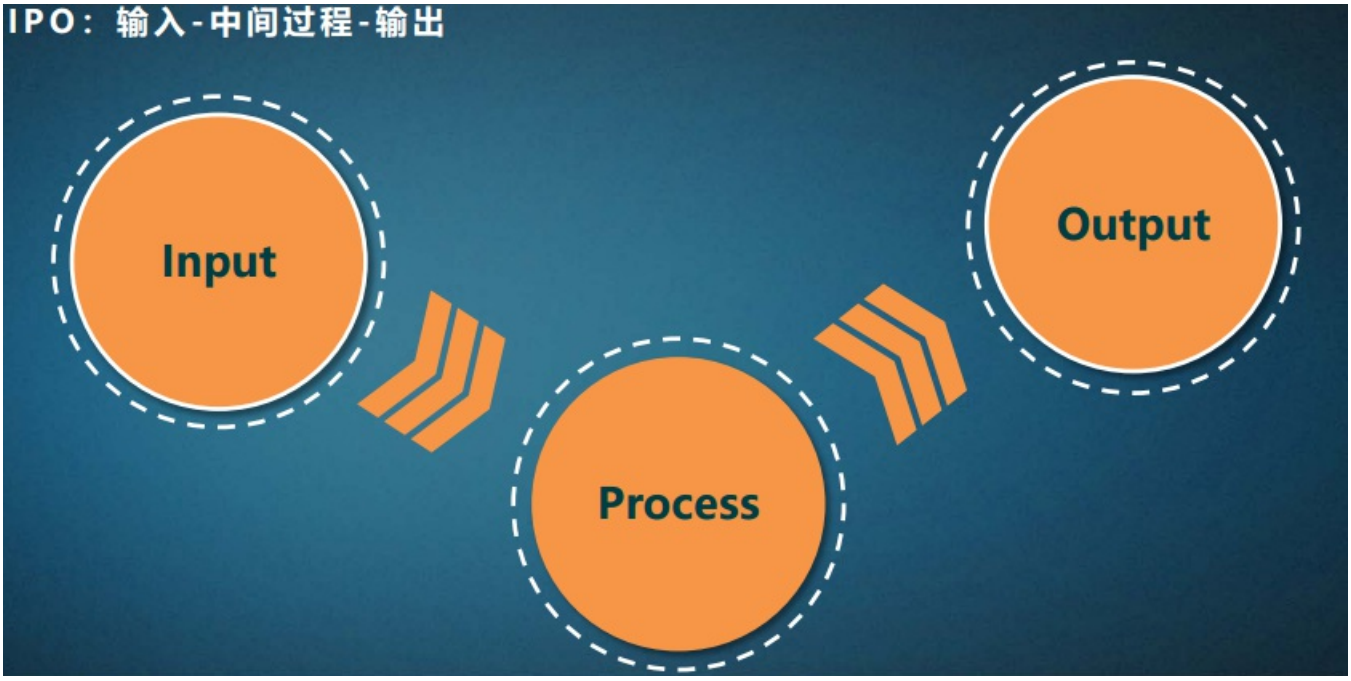
如今很大一部分人会通过游戏来进行适当的娱乐放松，在这个过程中玩家最关心的就是游戏的公平性问题，然而由于外挂的存在使得一些玩家轻轻松松就开启了“上帝模式”，因此如何反外挂就成了众多游戏公司最头疼的问题。腾讯游戏安全高级工程师胡和君在主题分享中，以FPS类型游戏的自瞄外挂功能的对抗为例，通过对自瞄外挂实现原理的解析，阐述了如何使用定制化的技术思想，达到对外挂作弊功能的持续压制。分享中还谈及游戏漏洞挖掘的核心思路和方法技巧，游戏开发者自身提升游戏安全性的技术手段，安全防守方定制化方案分析、开发、实现的方法和技巧等内容，相信能给相关工作者带来一定的启发。

腾讯游戏安全高级工程师胡和君

以下为演讲速记：

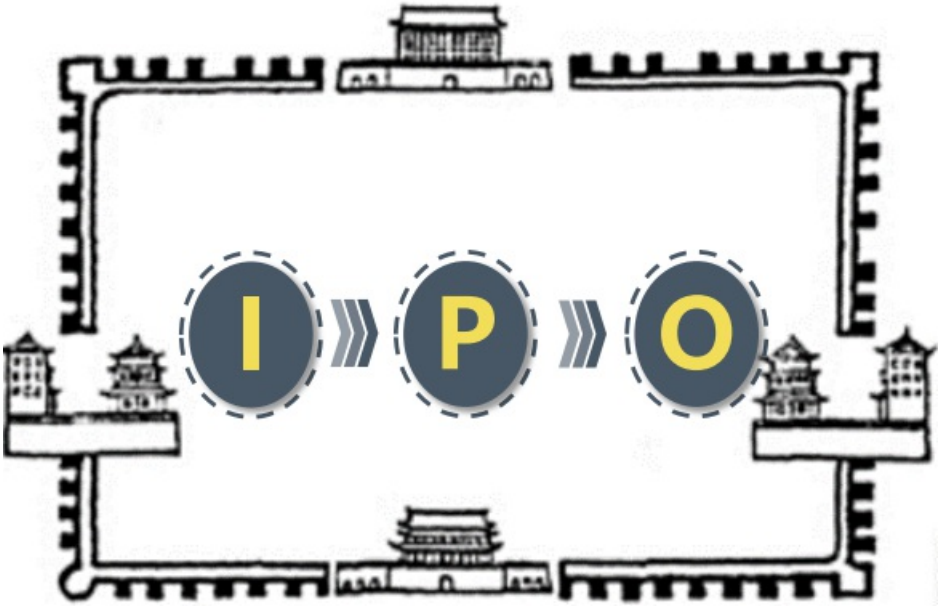
胡和君：大家好，今天我分享的议题是“定制化对抗——游戏反外挂的安全实践”。我来自腾讯游戏安全中心，09年就开始做穿越火线的外挂对抗，现在也是负责多款FPS类游戏的安全工作。与透视、自瞄这样的外挂功能对抗了8年，因此今天来分享一下在这8年的实践中，积累的一些解决思路。

游戏的抽象



定制化对抗是什么？大家先来看下一张图。这个图，就是三个字母，IPO。看着好像挺熟悉，想想也挺激动。可是我这里的这个IPO，并不是为了做公司上市的IPO，而是对游戏的一个抽象。游戏被抽象成什么呢？被抽象成为了一个输入，一个输出，和一个处理过程。游戏其实也就是通过一些输入，比如动动鼠标、敲敲键盘、划划屏幕、或是摇摇手机。然后通过游戏的一些逻辑或是处理流程，最终给到玩家一个反馈，比如移动了、攻击了、成功了、失败了、吃鸡了等等。而其实除了游戏以外，其他任何的虚拟世界的一个场景或是一个是业务都是可以被抽象成一个IPO的过程。而我们的安全问题，其实也就是和这个IPO过程相关。安全的问题，往往要么是制造一些非法的输入，比如通过精心构造的参数进行漏洞的触发和利用，要么是对中间过程进行一些篡改，比如病毒对系统的劫持感染，又或是对输出的结果的攻击，比如勒索病毒将正常的文件进行加密，或是诈骗木马将浏览器劫持访问一些非法的网站。而对于游戏来看，常见的一些外挂功能，比如模拟按键是针对输入的攻击、比如修改内存实现的秒杀无敌等功能是针对中间过程的攻击、而透视这样的外挂功能则是给游戏的输出进行了攻击，让你看到了本来不应该看到的东西。

通用的防御



而说道防御，通常的方案往往是铸建一个类似城墙的东西。把所有的各式各样的攻击拦截在外面，使得我们的游戏或是其他业务逻辑的IPO能够正常并顺利的运行下去。但是我们是知道的，天下没有不透风的墙。所以世上没有绝对的安全。那我们还可以怎么做呢？自然就是需要将防御方案深入到业务逻辑当中去，实施定制化的方案。假设右图是游戏逻辑的一个抽象，而所谓的定制化对抗，就是在除了外城的围墙以外，在具体的每个节点进行防御。而每个节点自身其实也就是一个IPO的过程。所以所谓定制化的对抗，就是从最小单元的IPO所展开进行的，在每一个游戏逻辑的节点以及游戏的路径上进行安全方案的防御和安全方案的部署。

定制化对抗

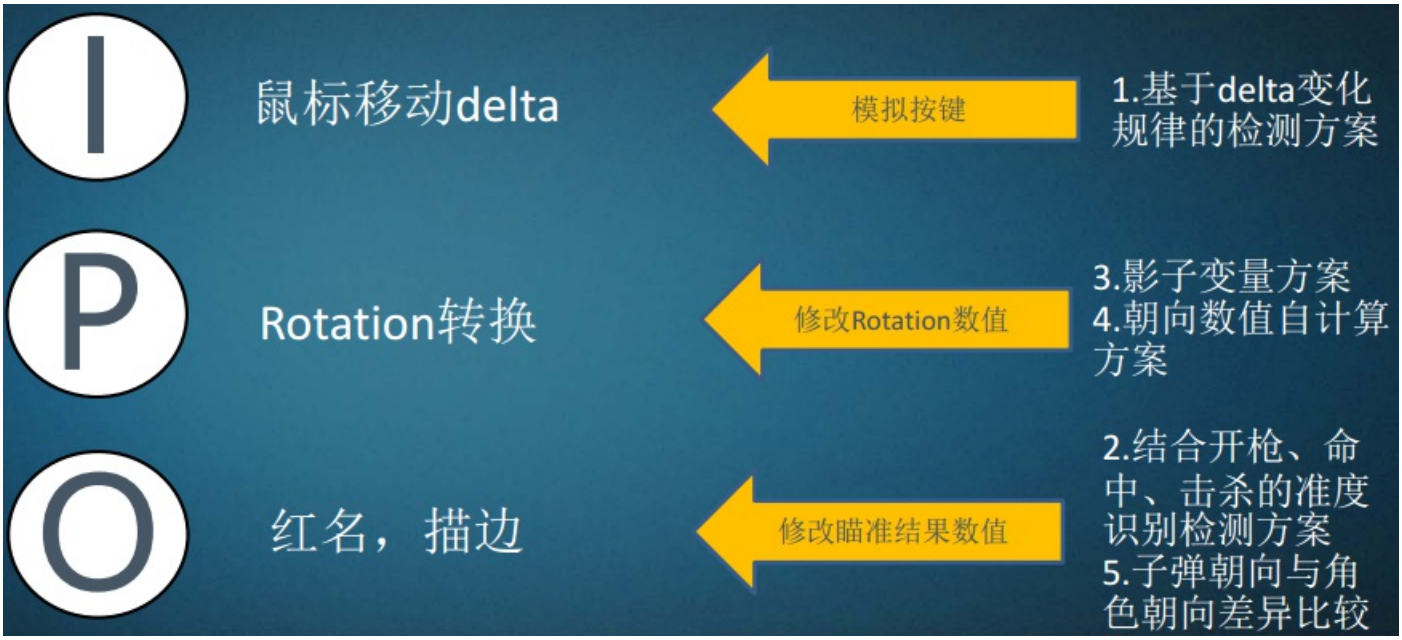
可能上面聊得还是比较虚，所以下面就用FPS类游戏常见的自瞄外挂对抗的一个例子，来介绍如何进行定制化方案的建设。因为要深入到游戏逻辑中去进行防御，因此我们先要对游戏自身的逻辑进行IPO的分解。其实游戏的瞄准逻辑非常容易理解，且很简单。其输入就是鼠标移动后的delta值，不同的游戏对这个delta值的处理不一样，而对FPS游戏来讲，其中间过程就是把鼠标这类设备输入的delta值转换为游戏逻辑中的Rotation，可以理解为一个朝向，如果形象一点来理解，可以把朝向认为就是现实生活中的脑袋。就是通过旋转脑袋来改变视野，而当瞄准以后，也就是所谓的输出，则往往是通过游戏内红名，或是人物描边等方式来展现。

基于游戏的逻辑

对游戏的逻辑进行拆分以后，自然攻击的方法，也就非常的明显。而我们防御手段则可以依据攻击方式进行见招拆招。如何见招拆招，实际就是找不同，针对攻击后的差异点分析。首先，来看看输入。直接秒想到的就是模拟按键。自瞄就是帮玩家瞄准，模拟按键就是一种帮忙的方式。而这种方式与正常的游戏有什么差异呢？最大的差别就是一种是真实按键，另一种是模拟按键。不过判断是否是真实安全的防御检测应该是外城墙所干的事情。那从结合业务逻辑的角度来看，又有什么差别呢？实际就是这个鼠标移动的delta值的变化规律。看看右图的示例，假设要想控制鼠标从A点移动到B点，对于模拟按键来看，这个变化规律是程一条直线，而人的正常移动则如第二个图所示，会有抖动，不是那么平滑。我们只要通过获取游戏的鼠标输入数据，然后对移动数值进行建模就可以识别出人与机器的差别。当然，模拟按键也可以模拟人的鼠标移动变得不是那么的平滑，但是从最终的数据表现来看，人的不确定性和外挂的相对稳定性是一个非常明显的差异。

在输入这一层找到差异后，继续往后，在中间过程这里，没有什么影响，模拟按键的方式很难影响游戏正常的Rotation转换过程。但是到了输出，也就是游戏的表现层。则是很明显自瞄的外挂比正常的玩家瞄得更准。而这个准如何去判断识别呢？可以从多个纬度去看，比如，因为瞄得准，因此杀人多，故KD比比较高，KD比也就是击杀和死亡比。又比如因为瞄得准，所以爆头率高。因为FPS游戏是两兵相遇准者活，这个准除了指能命中，更深入一点就是命中部位。因此也可以针对命中部位的聚集性进行建模。瞄得准，那他的命中部位是会有更明显的集中的。然而在这个过程中可能也会遇到职业玩家的挑战，因为水平高的玩家实际也就是瞄得准。所以接下来还需要看看正常瞄得准的和使用外挂瞄得准的差别，通过数据分析发现高手玩家瞄准和开枪这两个步骤是一气呵成的，非常连贯。但是作弊玩家这两个环节往往容易出现分离，也就是中间会有时差。总之就是按照找不同的方法去进行，一定可以发现作弊与非作弊的差异。

至此，模拟按键方式实现自瞄的找不同也就结束，对应的我们主要也就形成了基于delta的变化规律检测方案，结合击杀、命中部位、开枪时机等数据的准度识别检测方案。接下来我们再看看攻击方式，除了针对输入层进行攻击以外，针对中间过程也是一个很直接的攻击手段。大家也很容易想到，那就是可以通过修改内存，直接修改Rotation数值来达到瞄准的效果。



一样，我们也看看修改Rotation数值的方式在游戏逻辑侧有什么差别。从输入层来看，因为修改中间过程靠后因此对输入无影响。而从输出来看其实也就是和前面提到的模拟按键的最终效果一致。结合开枪、命中、击杀的准度识别检测方案也能够有所覆盖。而重点来看中间过程这里，实际最大的影响就是鼠标移动的delta到Rotation的计算结果发生了变化。这个计算结果怎么去防御呢？一种常见的检测方法就是进行影子变量的检测方案。将游戏计算的结果进行加密备份，在游戏使用的时候，把使用的数值与备份的解密数值进行比较。加密的原因是使得原始的数值在内存中不是那么容易的被发现。在这个过程中，如果发现数值有变化，表明了Rotation数值被进行了修改。当然这种方法会比较有效，但是也有弱点，一方面攻击者可以通过破解加密算法，而同时修改你备份的数值。另一方面攻击者可以直接修改计算逻辑，使得我们加密备份的数值自身就是游戏被修改过逻辑的代码所产生的，这样也就感知不到异常。所以一种相对更完备的方式则是进行Rotation的数值自计算。安全方案作为纯的旁入，获取鼠标移动的delta，然后通过与游戏同样的计算方式残生Rotation数值，最后对比数值的差异。而这种方案对逆向还原能力的要求是非常高的。对游戏中所有参与计算Rotation的逻辑都要进行精准的还原，否则就会导致方案的误判。这样针对修改Rotation的攻击方式，进行了三层的大家来找茬以后，整体又新增了影子变量与朝向数值自计算方案。

接着我们再来看针对输出层可以如何攻击。在这里实际就是直接修改瞄准的这个结果了。明明朝着门，确告知游戏瞄着人。这个相对而言更容易识别。只需要在开枪的时候，把子弹的朝向与角色的朝向进行对比就好了，因为如果不开枪，这种方式的作弊也没有任何收益。而但凡开枪，那么游戏中的异常表现就更是明显。越是表现层的差异，对游戏作弊发现来看越是容易进行检测。所以基于输入-中间过程-输出的方法，我们定制化的防御，就做到了以上5个基本方案的部署。

基于外挂的实现

然而，这并不算完成，除了知己还需要知彼。接下来需要从外挂功能实现的角度，再进行IPO的拆解，可以发现还有很多事情可以做。

从自瞄外挂的实现角度，很容易进行IPO的分解和对应。对应过来就是定位-换算-瞄准。瞄准其实就对应从游戏角度分析的攻击方式。所以这里主要就看看定位和换算。定位就是只要瞄准的目标在哪里？一般有两种方式，一种是通过屏幕取色，然后进行像素比对的方式发现目标。但其实这种方式在现有的外挂中并不常见，原因是并不好用，识别还是比较复杂的事情。比较好用的还是另一种方式，就是获取到目标在游戏内的坐标。然后到达第二步，进行换算，换算什么？就是计算鼠标移动的数值或是朝向瞄准的数值。在这个过程中会涉及游戏世界坐标系到屏幕坐标系的转换，转换为屏幕坐标以后，也就是可以得到当前鼠标与目标在屏幕上的关系如果是模拟按键则直接使用屏幕坐标可以计算出鼠标需要如何移动，而如果是修改朝向，则直接可以依据敌人坐标与自己的枪口坐标计算出命中射线的Rotation数值。

在对外挂实现方式的输入-中间过程-输出进行了分析以后，可以发现针对外挂的输入，我们可以进行坐标加密保护。其实这个更适合游戏开发方进行，而实际上我们防守方也是可以做，类似前面提到过的影子变量保护方案，我们对坐标的加密则是可以在游戏所有写的地方进行加密，然后在所有读的地方进行解密。而对于中间过程的换算，则是可以通过对游戏进行坐标转换的函数进行调用链回溯而发现，因为大部分的游戏世界坐标和屏幕坐标的转换都是有差异的。虽然外挂也可以自实现代码，但是当外挂自实现对应代码后，在内存中存在多份类似的代码，也是一种非常可疑的外挂特征。这样也就完成了对整个自瞄外挂知彼的分析和方案布防。再结合知己的视角所准备的5个基本方案。至此针对自瞄的外挂功能，从定制化的角度，就提出了以上的8个子方案，结业业务的逻辑进行安全对抗方案的布局。

定制化方案的成本

在实际的游戏反外挂实践中，腾讯的多款FPS类游戏都使用了以上的方案组合，基本实现了对自瞄类外挂的持续对抗。为什么叫持续对抗，因为游戏内容在不断的变化，玩家水平也在不断的变化，所以方案的模型也是持续的更新。这个也是定制化方案的一个成本，需要持续的维护，难以一劳永逸。而谈到成本，其实定制化方案最大的运营成本就是方案的适配。

适配是个什么东西？不是很好解释，先说说为什么需要适配。从定制化方案的建设来看，会在游戏的一些时机点获取游戏的数据。这些时机点和数据并不是游戏提供的，大部分情况下都是安全方进行的二次开发。其实也就是利用HOOK来实现。要么静态的patch到客户端，要么动态的HOOK的执行。而利用HOOK，那么也就会涉及到HOOK地址的问题，也包括函数头、函数尾、或是函数中间的选择。而获取数据的方式也就是依赖游戏自身的数据结构。这些都是通过逆向分析所得。而问题就是游戏版本是会持续变化的，所以这些我们所需要的地址和偏移也就是会变化的。所以适配也就是应对游戏的变化而对定制化方案所需要用到的地址和偏移进行修复。这里举一个适配的典型例子来说明适配的复杂度。假设一个函数原有逻辑是1，2，3。而我们的HOOK点就在3这个函数块。如果游戏逻辑发生了变化，在5这里多了一个分支，那其实对我们的方案来看是没有影响的，但是如果是出现图中4的方式，那么整个相关的游戏逻辑就需要重新分析和确认，因为有了分支4，原本通过3可以直接获取的数据或是感知的逻辑就不会走了。比如之前进行自瞄检测的影子变量的例子，这里多出来了一个对朝向数值的写，而我们没有能够及时对写的数据进行影子变量加密，那么在游戏正常读取的地方，则会认为读取到的数据和影子变量中的数值不匹配，从而带来方案的失效。除了适配，其实进行定制化对抗最大的成本还是在人。要做定制化的对抗，就需要对游戏非常的熟悉。这种熟悉除了玩游戏熟悉以外，更重要的是从逆向的角度对游戏非常熟悉。毕竟我们不是游戏开发，我们并没有游戏的代码，对游戏的理解都是依赖对游戏客户端的各种逆向分析所产生的结论和沉淀。与我们掌握一门技术类似，看过书和实践过是有较大的差别，同样一个游戏，自己比较完整的逆向分析过，和看过其他人的逆向分析报告是在不同的层次的。因此如果是一个新人接触一个新的游戏，都需要很长的一段时间来进行游戏逆向的积累，即使前人有较多的结论可供参考。而另外一个角度，一个老人如果还一个新的游戏，一样也是需要一段时间的积累，才能相对准确的把握到定制化方案。

定制化才能解决问题

虽然定制化的成本比较高，但是为什么我们还一直这么做，那确实是因为从目前的游戏外挂对抗来看，只有定制化的对抗方式才能解决问题。这里的解决并不是指完全的消失，而是能够做到一种及时的压制。对比没有定制化逻辑的其他反外挂系统来看，确实是有他的效果。虽然定制化的成本比较高，但是我们知道安全需求是属于人类需求的低级需求，作为低级需求那就是必须要保障的。因此只要能够解决安全的问题，不论成本多大，都是值得的。而所谓成本和效率则是在解决问题的基础上再谈的话题了。

而从目前来看，安全的问题越来越复杂，很难有通用的方法能够搞定一切，而越是通用的方案越容易被针对，因此个人认为定制化的对抗方式，就如同定制化的商品一样，贵，但是能更贴合的满足客户的需求。而自己也认为IPO的方式，除了对游戏安全有效果，对其他的业务安全场景也会有帮助。

我的分享到这里结束了，主要分享一下我们定制化方案实践的IPO之路，谢谢大家。

> 注：本文根据大会主办方提供的速记整理而成，不代表CSDN观点。

2017看雪安全开发者峰会更多精彩内容：

- 2017看雪安全开发者峰会在京召开 共商网络安全保障之策
- 中国信息安全测评中心总工程师王军：用技术实现国家的网络强国梦
- 兴华永恒公司CSO仙果：Flash之殇—漏洞之王Flash Player的末路
- 中国婚博会PHP高级工程师、安全顾问汤青松：浅析Web安全编程
- 威胁猎人产品总监彭巍：业务安全发展趋势及对安全研发的挑战
- 启明星辰ADLab西南团队负责人王东：智能化的安全——设备&应用&ICS
- 自由Android安全研究员陈愉鑫：移动App灰色产业案例分析与防范
- 腾讯反病毒实验室安全研究员杨经宇：开启IoT设备的上帝模式
- 绿盟科技应急响应中心安全研究员邓永凯：那些年，你怎么写总会出现的漏洞
- 绿盟科技网络安全攻防实验室安全研究员廖新喜：Java JSON 反序列化之殇
- 阿里安全IoT安全研究团队Leader谢君：如何黑掉无人机