看雪 2017 安全开发者峰会

Kanxue 2017 Security Developer Summit

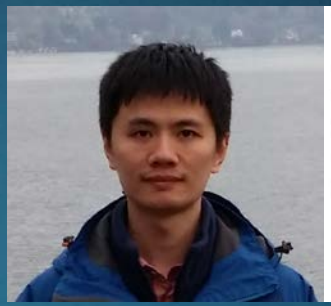
2000-2017

定制化对抗——游戏反外挂的安全实践

胡和君 腾讯科技 游戏安全中心

自我介绍

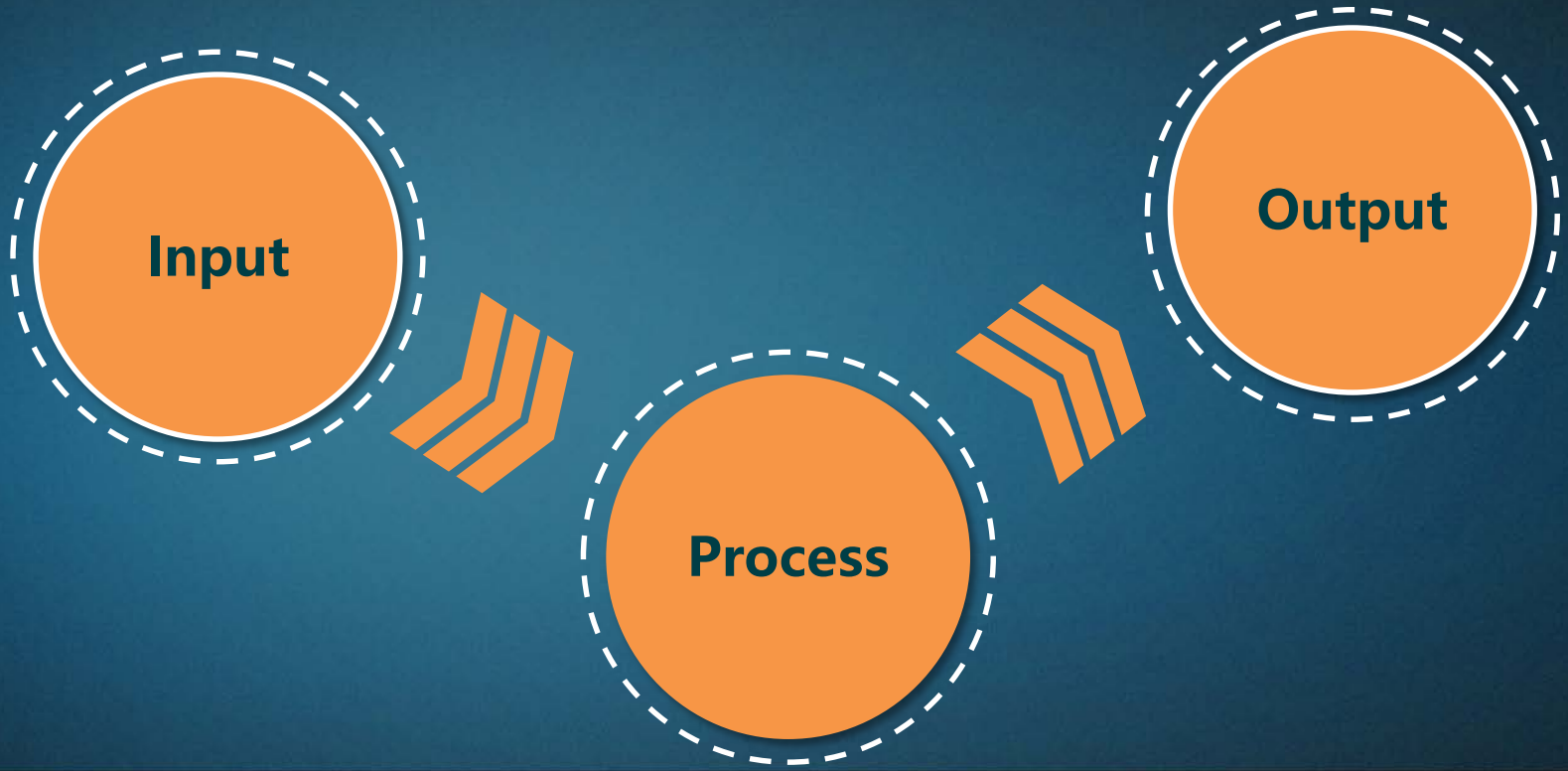
胡和君



- 游戏安全高级工程师
- 就职于腾讯游戏安全中心
- 负责FPS类游戏安全对抗工作
- 从事PC端游戏安全相关工作8年
- 涉及游戏安全评审、游戏外挂分析与对抗、游戏漏洞分析与应对、安全方案开发

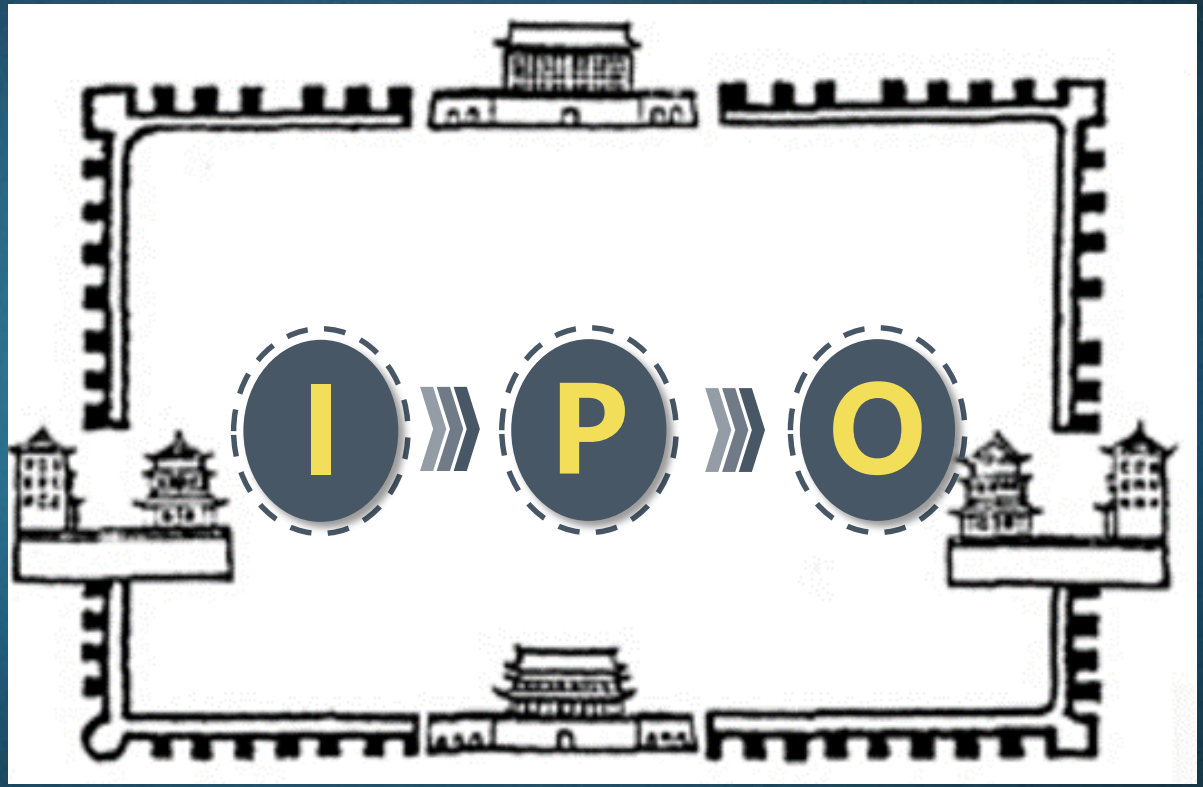
游戏的抽象

IPO：输入-中间过程-输出



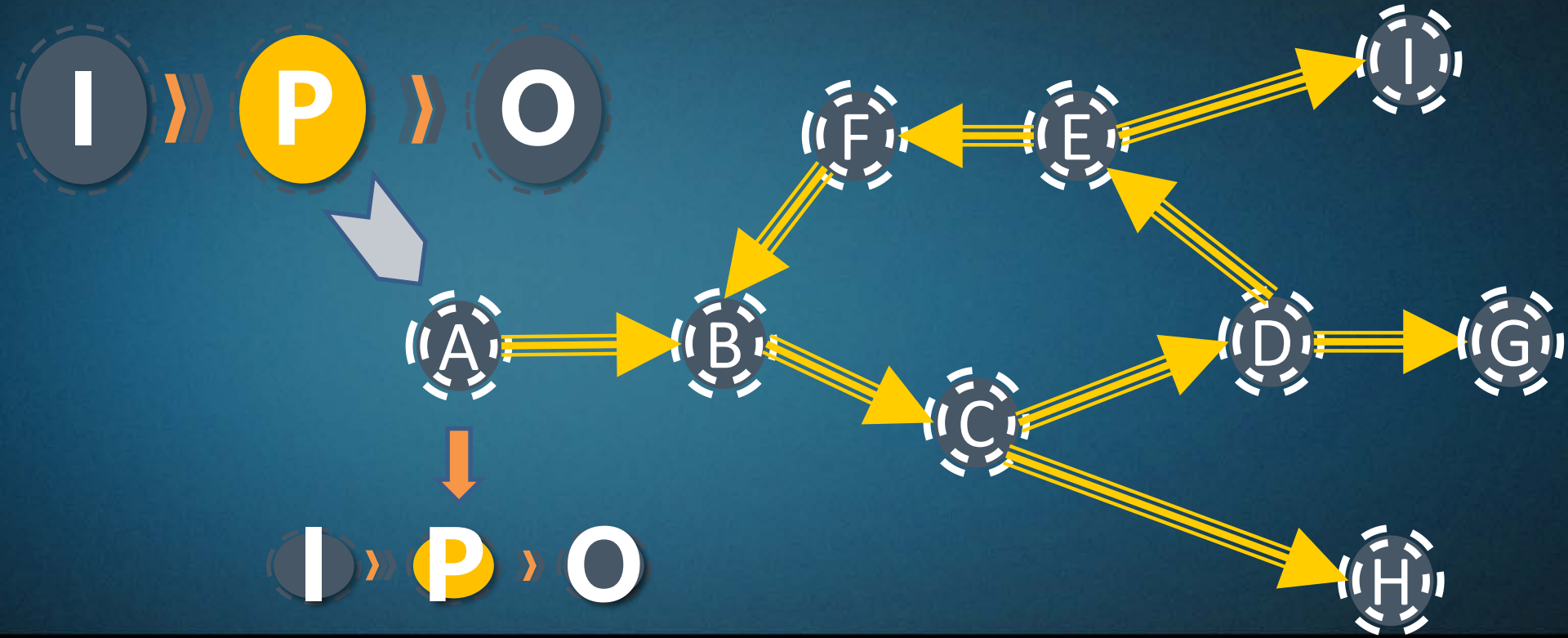
通用的防御

天下没有不透风的墙

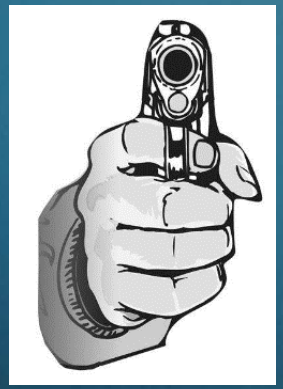


定制化对抗

深入业务逻辑的防御方案



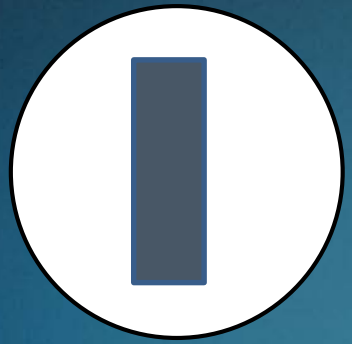
AUTO AIM



定制化对抗

IPO-基于游戏的逻辑

游戏的瞄准逻辑



输入

鼠标移动
delta

中间过程

Rotation
转换

输出

红名、描边
高亮等

定制化对抗

IPO-基于游戏的逻辑

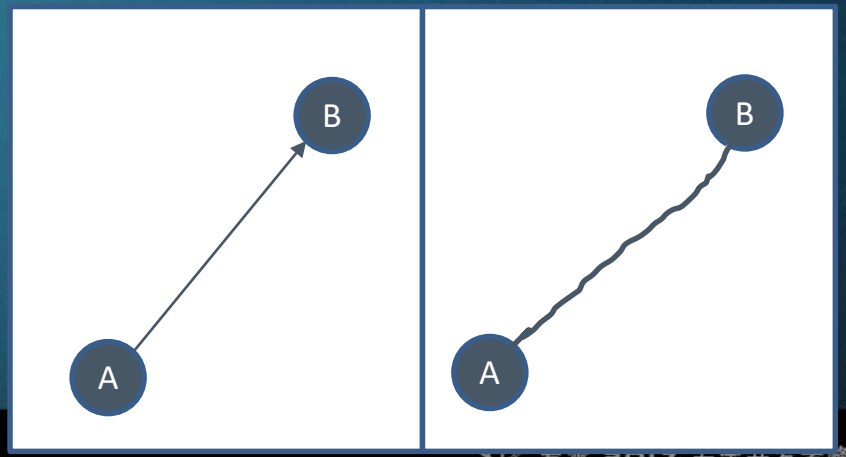
I

鼠标移动delta

模拟按键

P

Rotation转换



O

红名，描边

定制化对抗

IPO-基于游戏的逻辑

鼠标移动delta

Rotation转换

红名，描边

模拟按键

delta平滑

无差别

变准

KD比
爆头率
命中率
连贯性
等等...

定制化对抗

IPO-基于游戏的逻辑

鼠标移动delta

模拟按键

基于delta变化规律的检测方案

Rotation转换

修改Rotation数值

红名，描边

结合开枪、命中、击杀的准度识别检测方案

定制化对抗

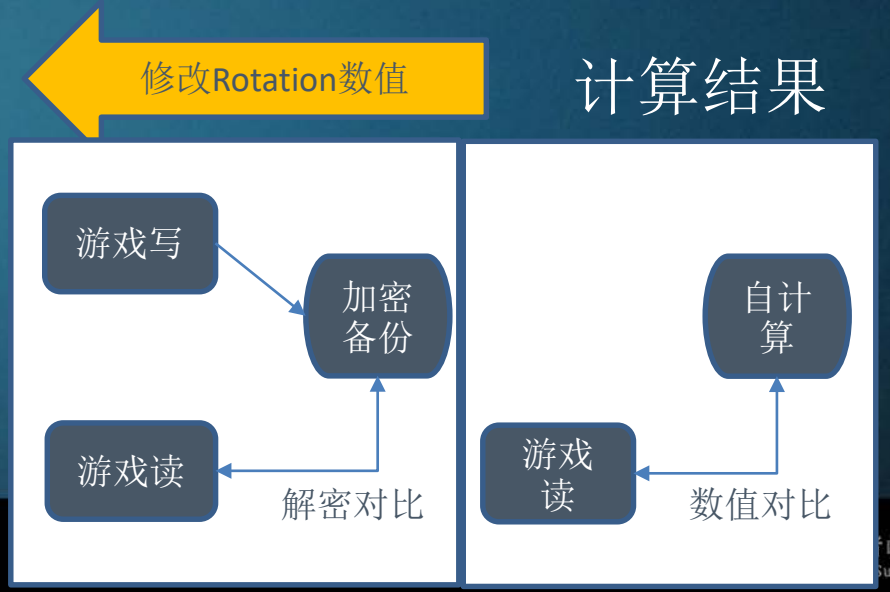
IPO-基于游戏的逻辑

I 鼠标移动delta

P Rotation转换

O 红名，描边

无差别



定制化对抗

IPO-基于游戏的逻辑

I

鼠标移动delta

模拟按键

1.基于delta变化规律的检测方案

P

Rotation转换

修改Rotation数值

3.影子变量方案

4.朝向数值自计算方案

O

红名，描边

2.结合开枪、命中、击杀的准度识别检测方案

定制化对抗

IPO-基于游戏的逻辑

鼠标移动delta

模拟按键

1.基于delta变化规律的检测方案

Rotation转换

修改Rotation数值

3.影子变量方案
4.朝向数值自计算方案

红名，描边

修改瞄准结果数值

2.结合开枪、命中、击杀的准度识别检测方案
5.子弹朝向与角色朝向差异比较

定制化对抗

IPO-基于外挂的实现

知己知彼百战不殆

定制化对抗

IPO-基于外挂的实现

I

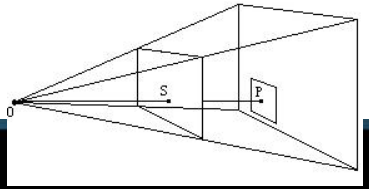
定位

获取坐标
或
图像识别

P

换算

鼠标移动数值
或
游戏朝向数值



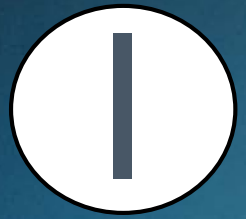
O

瞄准

模拟鼠标移动
或
修改朝向数值

定制化对抗

IPO-基于外挂的实现



定位

1.坐标加密

换算

2.世界坐标系->屏幕坐标系的调用链回溯
3.游戏关键函数特征的内存扫描

瞄准

4.基于delta变化规律的检测方案
5.结合开枪、命中、击杀的准度识别检测方案
6.影子变量方案
7.朝向数值自计算方案
8.子弹朝向与角色朝向差异比较

定制化对抗

成本

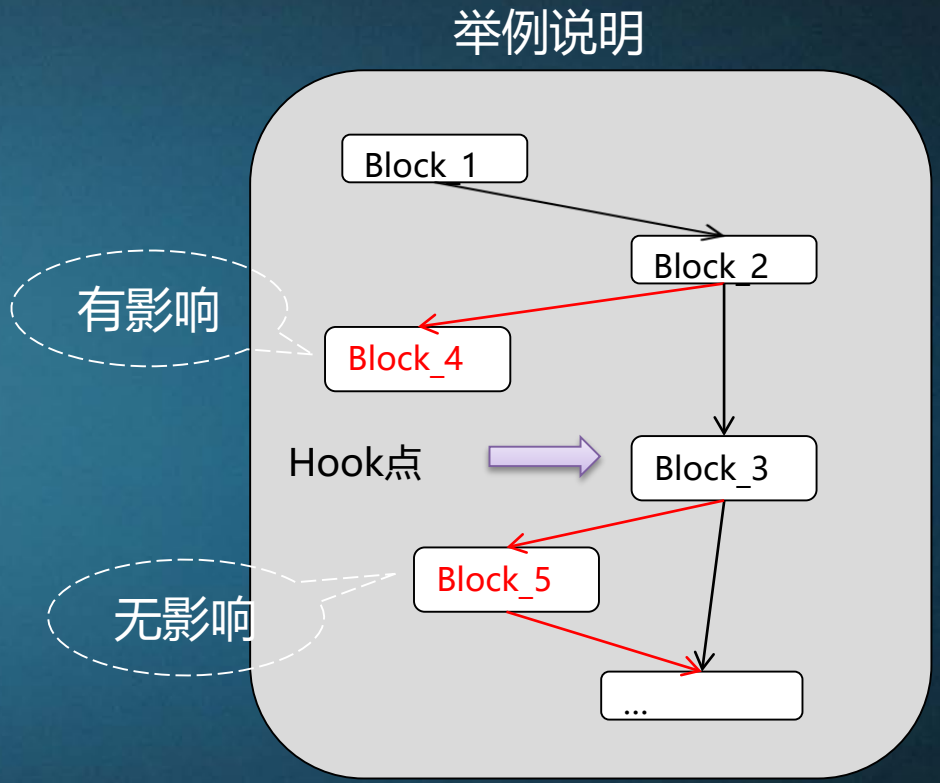
定制化方案的成本

定制化对抗

适配成本

适配

Address + Offset



定制化对抗

人力成本

定制化对抗

定制化才能解决问题

安全问题是
必须要解决的问题

The War Never End