MY.GAMES

СЕРВЕРНЫЙ АНТИЧИТ: ПАНАЦЕЯ ИЛИ РУДИМЕНТ?

Евгений Ченцов, программист

Евгений Крутских, старший QA-специалист

КТО МЫ? IT TERRITORY!

16 лет

16 игр

250 человек

100 000 000 игроков

ПЛАН

- Актуальность проблемы читов
- Античит и сервер
- Серверный антиспидхак и его тестирование
- Дополнение серверной защиты
- О рекомендациях и их упорном игнорировании

ДУМАЕТЕ, ЭТО ВАС НЕ КАСАЕТСЯ?

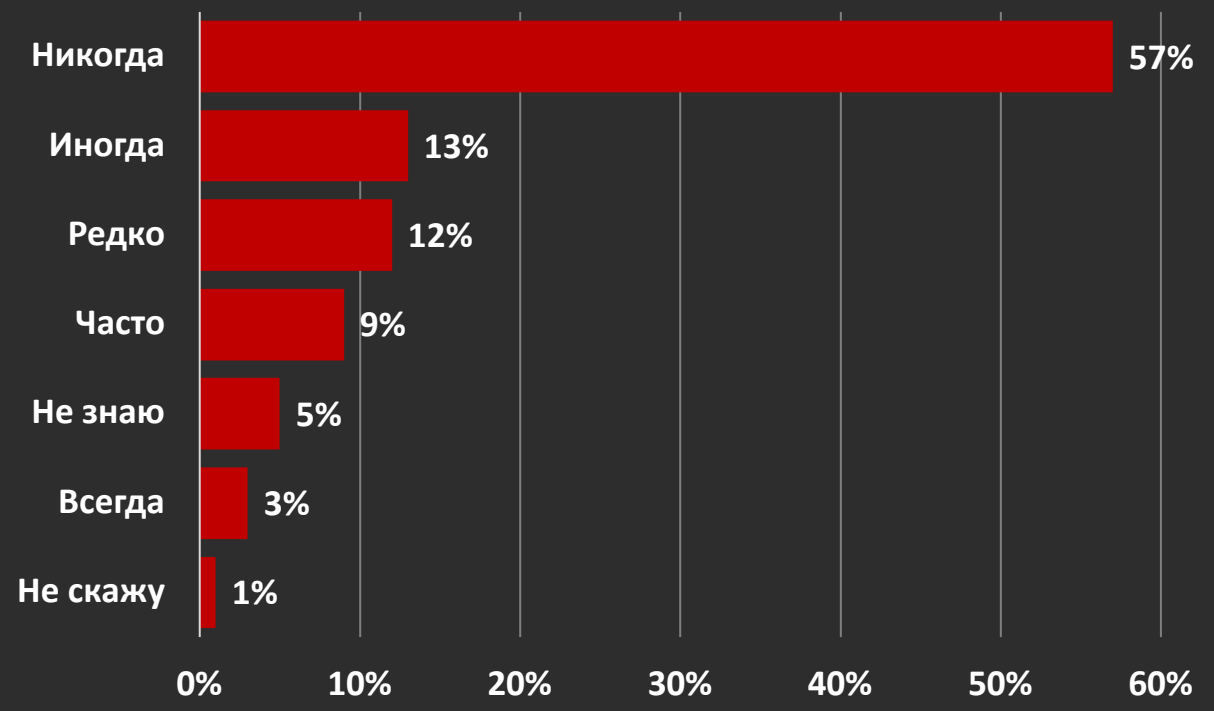
тогда мы идем к вам!

СКОЛЬКО ЧИТЕРОВ?

37%

игроков хотя бы раз применяли читы

«Как часто вы используете стороннее ПО для читов в мультиплеерных играх?»



Данные: irdeto.com, 2018

КАКОВО ВЛИЯНИЕ?

MY.GAMES

60%

игроков испытали негативный опыт от игры с читерами

76%

респондентов считают, что онлайн игра должна быть защищена от читов

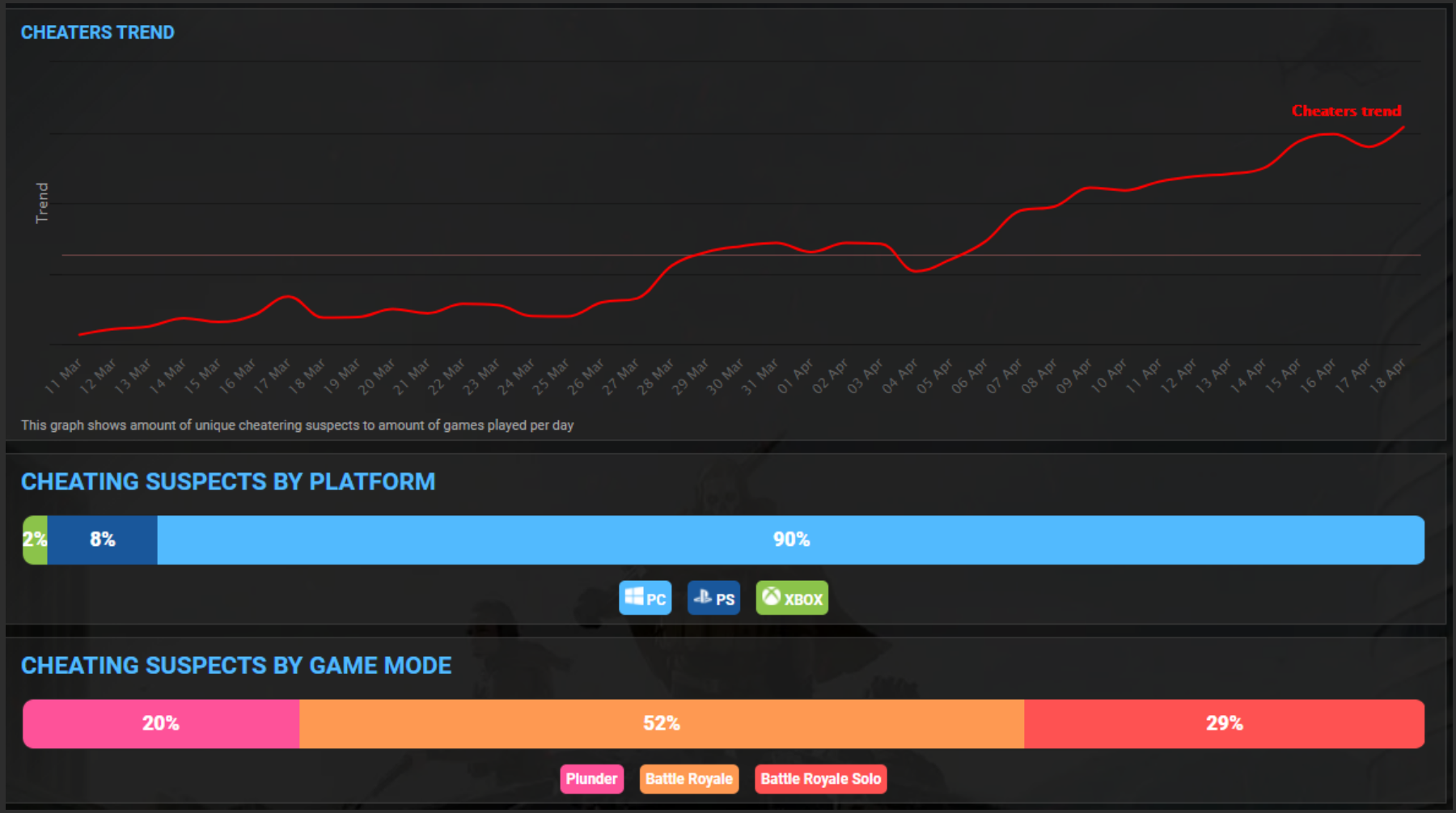
48%

игроков покупали меньше внутриигрового контента, если сталкивались с читерами в игре

Данные: irdeto.com, 2018

СТАТИСТИКА

Call of Duty



Данные: codstats.net, 2020

ПРИЧИНЫ ИСПОЛЬЗОВАНИЯ

- Ускорение прокачки
- Получение платного контента
- Обход игровых ограничений «для получения удовольствия»
- Осознание игрового преимущества над другими игроками

Вопрос, который задает себе каждый игрок перед включением чита:

«А что мне за это будет?»

ПРИЧИНЫ РАЗВИТИЯ СФЕРЫ

2.5

млн. долларов США принес разработчику бот ***WoWGlider*** **(**kaspersky.com, 2018**)**

7 500

долларов США в месяц зарабатывает разработчик читов для популярной FPS игры (bbc.com, 2019)

КЛАССИФИКАЦИЯ АНТИЧИТОВ

- **Клиентские** (защита игрового клиента от внешних вмешательств)
- **Серверные** (валидация данных на сервере)
- **Статистические** (анализ игровых результатов постфактум)
- **Система репортов**
- **Геймметаника** (защита на уровне игрового дизайна)

СЕРВЕР + АНТИЧИТ?

- Данные на сервере невозможно подменить
- Следовательно, серверным данным можно доверять
- И, поведение объектов можно проверять!
- Всегда ли можно провести точный анализ ***поведения***, имея данные?
- Сервер слеп без клиента. Сильно ли?
- **КАК ЭТО ТЕСТИРОВАТЬ?**

СЕРВЕРНЫЙ АНТИСПИДХАК

Условия:

- Новая мультиплеерная игра
- Игрок управляет персонажем в трехмерном мире
- На момент релиза **нет** сложных механик движения
- Мы хотим отдать на бой **полностью рабочее решение**

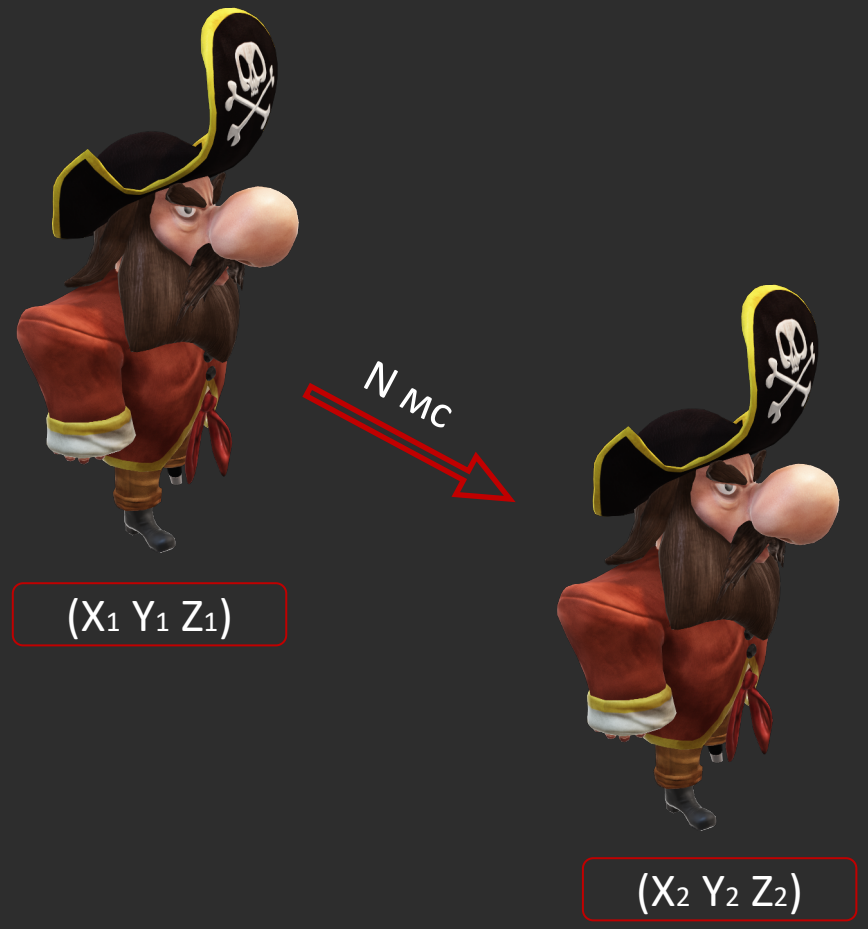
СЕРВЕРНЫЙ АНТИСПИДХАК

СЕРВЕРНЫЙ АНТИСПИДХАК

ДИСКЛЕЙМЕР

- Это всего лишь абстрактный пример!
- Ваша команда наверняка находится в условиях, отличных от условий в данном примере
- Не все проекты обладают механиками перемещения, описанными далее
- А реализация других механик может быть и простой, и эффективной

РЕАЛИЗАЦИЯ-1



- Сервер хранит информацию о старых координатах
- Спустя N миллисекунд на сервер приходит информация о новых координатах персонажа
- Скорость вычисляется как длина прямой между двумя координатами, которая делится на время
- Если вычисленная скорость превышает некоторое заданное значение, срабатывает защита и применяется какая-то ***санкция***

ТИПЫ САНКЦИЙ

- **Локальный** (возвращение на предыдущую точку)
- **Умеренный** (внутриигровые ограничения)
- **Скрытый** (последствия не очевидны игроку)
- **Жесткий** (кик, бан)

КРИТЕРИИ ВЫБОРА

- **Вероятность ошибки** в определении факта нарушения
- **Игровая политика**
- **Тип игры**

РЕАЛИЗАЦИЯ-1. ТЕСТЫ

Вариант плохой:

Прямая проверка алгоритма

X=0	Y=0	Z=0	T=0	PASS
X=0	Y=1	Z=1	T=1	

X=0	Y=0	Z=0	T=0	PASS
X=15	Y=-30	Z=12	T=0.5	
X=0	Y=1	Z=1	T=1	

Вариант получше:

Суммируем расстояние по всем точкам в промежутке [0, 1]

X=0	Y=0	Z=0	T=0	FAIL
X=15	Y=-30	Z=12	T=1	

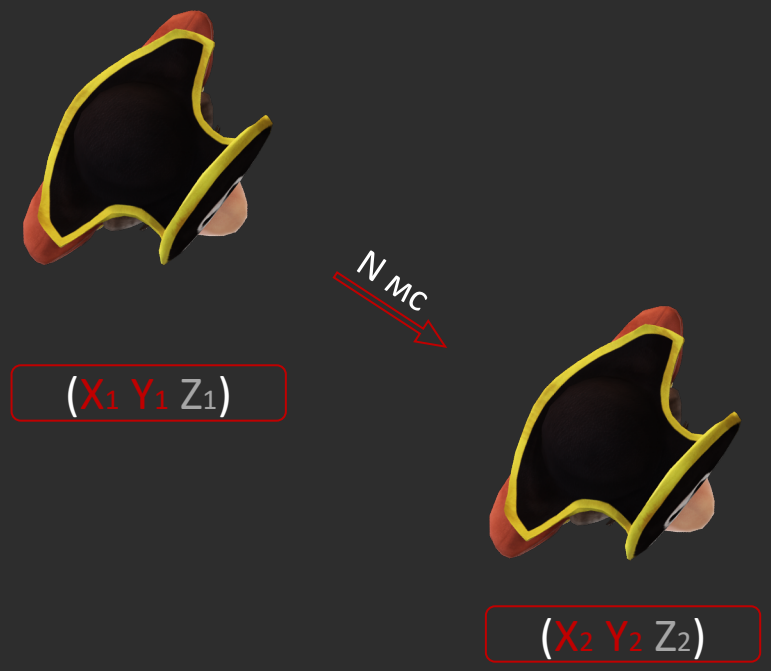
X=0	Y=0	Z=0	T=0	FAIL ???
X=15	Y=-30	Z=12	T= 0.5	
X=0	Y=1	Z=1	T=1	

РЕАЛИЗАЦИЯ-1. ВЫВОД

- Вычисление скорости только за промежуток времени приводит к большим погрешностям
- Расчет пройденного расстояния по трем координатам – не всегда хорошая идея

Итог: подобная идея неработоспособна

РЕАЛИЗАЦИЯ-2



Что делаем:

- Избавляемся от Z координаты
- Храним историю перемещений

Проблемы и вопросы:

- Нужно делать защиту от полетов
- Как долго хранить информацию о перемещении?

РЕАЛИЗАЦИЯ-2. ТЕСТЫ

- Копим историю из **N=3** точек. Применяем санкцию при превышении **Vcp**

X=0	Y=0	Z=0	T=0
X=1	Y=1	Z=100	T=0.5
X=2	Y=1	Z=1	T=1

PASS

X=0	Y=0	Z=0	T=0
X=1	Y=1	Z=100	T=0.5
X=15	Y-30	Z=12	T=1

FAIL

X=0	Y=0	Z=0	T=0
X=15	Y=-30	Z=12	T=0.5
X=0	Y=1	Z=0.5	T=1

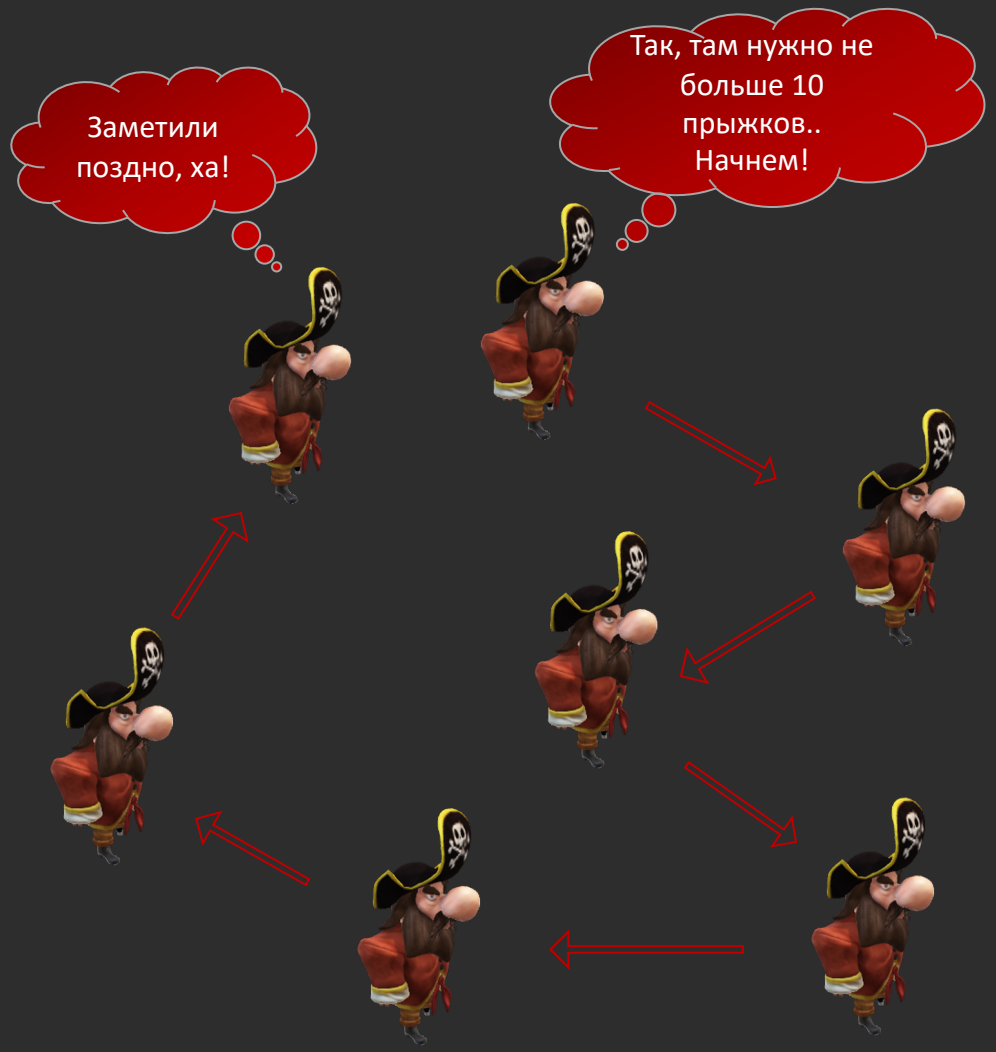
FAIL

Все ли хорошо
в этих тестах?

CHEATER STRIKES BACK

MY.GAMES

РЕАЛИЗАЦИЯ-2. ВЗЛОМ



Пример атаки: нарушать до накопления нужного количества точек

Результат:

возможность телепортации в любую точку карты

РЕАЛИЗАЦИЯ-3

- **Источник проблем** – необходимость накопления истории перемещения
- Ставим ограничение на расстояние персонажа между двумя тиками (задание максимально возможного шага) и сочетаем его с историей
- Получаем проверку **мгновенной** и **средней** скорости

РЕАЛИЗАЦИЯ-3. ТЕСТЫ

- Копим историю из **N=3** точек. Применяем санкцию при превышении **Vmax**

X=0	Y=0	T=0	PASS
X=1	Y=1	T=0.5	
X=2	Y=1	T=1	

X=0	Y=0	T=0	FAIL
X=15	Y=-30	T=0.5	
X=0	Y=1	T=1	

X=0	Y=0	T=0	FAIL
X=1	Y=1	T=0.5	
X=15	Y-30	T=1	

X=0	Y=0	T=0	PASS
X=0	Y=1	T=1	

X=0	Y=0	T=0	FAIL
X=15	Y-30	T=1	

NETWORK STRIKES BACK

MY.GAMES

РЕАЛИЗАЦИЯ-3. ПОЛОМ

“Network strikes back”

- **Проблема**: лагающая сеть
- Данные от клиента нестабильно приходят на сервер -> возникает ложноположительное срабатывание
- **Дополнительная проблема**: какова политика игры по отношению к лагерам?

РЕАЛИЗАЦИЯ-4

- Чаще всего в играх задана относительно ***мягкая политика*** по отношению к «умеренным лагерам»
- ***Что делаем***: вводим амортизацию перемещения
- Поправку на лаг нужно учитывать и при ***расчете скорости*** (изменение алгоритма расчета), и при ***анализе длины шага*** (увеличение порога)

DESIGNER STRIKES BACK

MY.GAMES

РЕАЛИЗАЦИЯ-4. ПОЛОМ

Одел сапоги-скороходы и увеличил скорость на 20%

Выпил волшебное зелье и стал бегать в два раза быстрее на 10 секунд

Выучил заклинание коротких телепортов и стал дэшить налево и направо

Изначально вам говорили, что сложных механик движения в игре нет…

…ТЕПЕРЬ ОНИ ПОЯВИЛИСЬ

РЕАЛИЗАЦИЯ-5

- Механики, изменяющие скорость игрока, должны также изменять и верхний предел скорости
- Определяется некий максимальный уровень скорости, выше которого предел вырасти не может
- Для различного транспорта изменение скорости задается аналогично, но верхний предел скорости, возможно, также придется корректировать

РЕАЛИЗАЦИЯ-5. ТЕСТЫ

- Копим историю из **N=3** точек. Применяем санкцию при превышении **Vmax**

V=1	T=0	Vmax=2	PASS
V=3	T=0.5	Vmax=3	
V=4	T=1	Vmax=4	

V=1	T=0	Vmax=2	FAIL
V=3	T=0.5	Vmax=4	
V=2	T=1	Vmax=2	

V=1	T=0	Vmax=2	FAIL
V=3	T=0.5	Vmax=4	
V=4	T=1	Vmax=2	

РЕАЛИЗАЦИЯ-5

В предложенной реализации нельзя мгновенно изменять верхний предел скорости

Шаг в истории	V средняя, м/с	Предел скорости, м/с
1 (простой бег)	15	20
2 (простой бег)	16	20
3 (одел сапоги)	21	21
4 (+ выпил зелье)	40	40
5 (- зелье)	22	21
6 (снял сапоги)	21	20

ОТНОСИТЕЛЬНЫЕ КООРДИНАТЫ

Скорость относительно корабля: 0 м/с

Скорость относительно острова: 50 м/с

- Перемещение персонажа нужно измерять в ***относительных координатах***
- Проблемы могут возникнуть ***при переходе к другой системе координат***

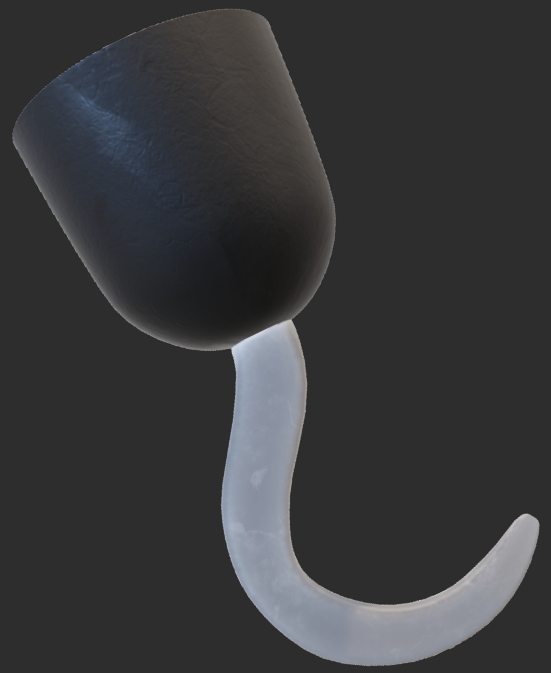
ТЕСТИРУЕМ. ЮНИТ ТЕСТЫ

- Замыкают логику работы алгоритма в уме разработчика (сам написал, сам проверил)

- При отсутствии документации не имеют ценности для оценки поведения

+ Все еще жизненно необходимы

ТЕСТИРУЕМ. РУЧНЫЕ ПРОВЕРКИ



+ Заставляют разработчика описывать алгоритм так, чтобы его мог понять QA

+ Позволяют тестировать не набор данных, а ***поведение***

- Крайне трудоемки – очень много сценариев

- Человеческий фактор

ТЕСТИРУЕМ ШИРЕ. РЕГРЕСС БОТЫ

+ Заставляют разработчика описывать алгоритм так, чтобы его мог понять QA

+ Позволяют тестировать не набор данных, а ***поведение***

+ Без устали проверяют все сценарии нестандартного поведения персонажа после каждой правки

- Для больших проектов реализация кастомных ботов – дорогая задумка. Очень дорогая.

РЕГРЕСС БОТЫ. УСТРОЙСТВО

- Бот представляет собой «пустого» персонажа в игре
- Поведение бота задается с помощью набора действий. Функционал позволяет реализовать и действия, выходящие за рамки возможностей игрока
- Последовательность действий становится сценарием, регулярно прогоняемым на билдере

РЕГРЕСС БОТЫ. МЕЧТА

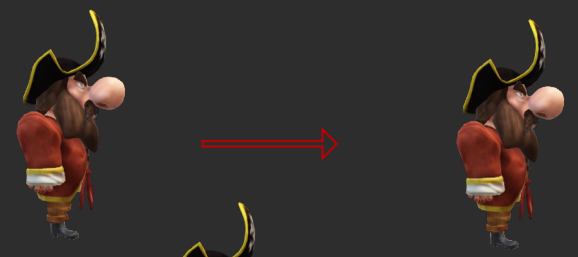
1. Телепортироваться в точку 1
2. Задать максимальную честную скорость
4. Стартовать таймер
5. Дойти до точки 2
6. Зафиксировать время таймера (T0)

7. Телепортироваться в точку 1
8. Задать читовую скорость
10. Стартовать таймер
11. Дойти до точки 2
12. Зафиксировать время таймера (T1)

T0 < T1?

ТЕЛЕПОРТАЦИЯ И ЕЕ ВИДЫ

- Дэш



- Телепорт в рамках карты

- Телепорт между картами

- Когда телепортируемся далеко – историю перемещения нужно сбросить

ВОПРОС ВЕКА

Является ли телепортация **единственным** случаем, когда необходимо сбрасывать историю?

В идеальном мире – да.

Но мы не там!

ДЛИННЫЕ ПРЫЖКИ. ПРИМЕР

ДЛИННЫЕ ПРЫЖКИ

Длинные прыжки могут быть:

- очень длинными (до 100-150 метров)
- очень быстрыми (до 3х-4х от максимальной скорости персонажа)
- очень высокими (ограничения на высоту нет)
- связаны с перемещением между взаимно перемещающихся объектов

- Прыжки имеют прогнозируемую длительность

- Нужно ли специально обрабатывать такой случай?

ДЛИННЫЕ ПРЫЖКИ. АТАКА

Если защиту не делать:

- В момент полета можно подменять координаты (пока происходит длинный прыжок)

Если реализовать защиту через сброс истории:

- Можно найти способ злоупотребления сброса истории

- Существует значительное количество вариаций атак при выборе второго варианта защиты

ДЛИННЫЕ ПРЫЖКИ. ЗАЩИТА

- Длительность прыжка ***<u>учитывается в механике</u>***. Нельзя продлевать длительность ее работы
- Во время «нестандартной» работы механики защиты остаются, пусть и имеют другие значения
- Учитываем влияние истории перемещения после окончания работы прыжка
- Трейд-офф: сложная внутренняя реализация

ЛОЖНЫЕ ПАКЕТЫ. АТАКА

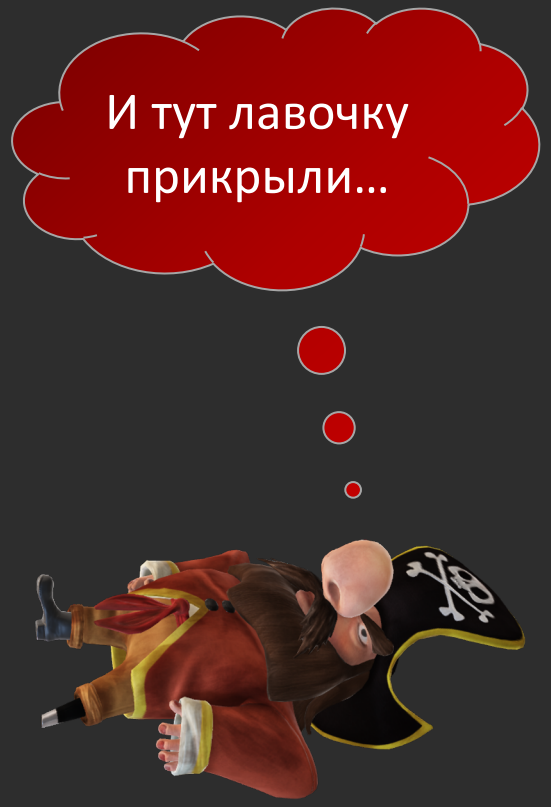
Суть атаки: искажение информации, которая попадает в историю

Методы:

- многократная отправка пакетов на сервер
- особый способ отправки пакетов (отложенная отправка, повторная отправка, комбинация)
- подобные атаки особенно эффективны при небольшой истории перемещения

ЛОЖНЫЕ ПАКЕТЫ. ПРИМЕР

ЛОЖНЫЕ ПАКЕТЫ. ЗАЩИТА



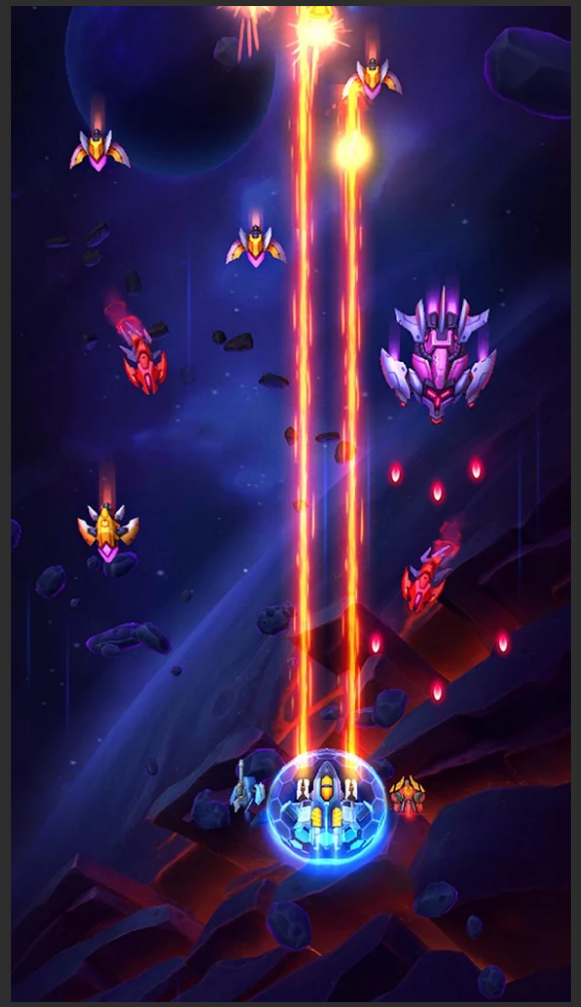
- **Считаем** количество получаемых пакетов с учетом особенностей работы клиента
- **Анализируем** полученные пакеты с точки зрения целесообразности записи информации
- Особенно внимательно анализируем имеющиеся по нарушению данные для тюнинга

О ЛОЖНОПОЛОЖИТЕЛЬНОМ

- Ложноположительные срабатывания **неизбежны**
- Слишком частые срабатывания приводят к негативному игровому опыту
- Слишком редкие срабатывания **не указывают** на эффективность работы.
- Грамотный выбор санкции очень важен
- Хорошая практика перед ужесточением санкций – применение их не на всей аудитории проекта

О ЛОЖНОПОЛОЖИТЕЛЬНОМ

Space Justice



СЕРВЕР. АНТИЧИТ. РЕЗЮМЕ

- Наличие серверной защиты значительно усиливает позиции античита
- Использование серверной защиты не является гарантией отсутствия читов
- Сложные игровые механики скорее всего приведут к компромиссным решениям при проектировании защиты и увеличению стоимости ее обслуживания

- *Вот бы реализовать систему, в которой серверу будут **активно помогать**...*

ЗАЩИТА КЛИЕНТА

- Клиент – «глаза сервера, которые могут лгать»
- Клиентский античит усложняет задачу разработчиков читов
- Клиентский античит без дополнительной защиты имеет большое количество уязвимых мест

ГЕЙМДИЗАЙН

- Уязвимости игровой механики – не задача античита
- Дизайн игровых механик напрямую влияет на поддержку систем защиты (например, туман войны в Dota 2)
- Проблемы на грани между игровой механикой и античитом чаще решаются с помощью дизайна
- Сложные решения на уровне геймдизайна – явный намек на наличие «костылей»?

ГЕЙМДИЗАЙН. ПРИМЕРЫ

Space Justice: Saint Patrick’s day

- Валидация получения максимального количества золота за раунд происходит на сервере
- **Суть**: появляется возможность с некоторой вероятностью увеличить количество получаемого золота
- **Проблема**: Дизайн изменился, защита от взлома валюты – нет.
- **Решения**:
  1. Изменить дизайн и/или доработать проверку валидации
  2. Доработать взаимодействие «дизайнер – программист»

СТАТИСТИКА И АНТИЧИТ

Идея: анализировать статистические показатели игрока для выявления аномального поведения

Преимущества:

- Нет завязки на клиент. Анализируется фактическая информация
- Аномальное поведение достаточно легко определяется. Легко находятся «неумные» читеры

Недостатки:

- Сложности при пограничных случаях («умный» читер)
- Читеры находятся постфактум (нарушение уже произошло)

ИТОГИ

- Серверный античит – **must have** для проекта с наличием серверной логики
- Клиентский античит – **must have** для любого онлайн-проекта
- Прислушивайтесь к сообществу – игроки знают ситуацию лучше разработчиков
- Для бесплатных игр нужен барьер, не позволяющий делать много регистраций
- Привлекайте дизайнеров к любым задачам с читами - возможно, их решение будет изящнее вашего
- Используйте статистику. Развивайте инструменты ее анализа

P.S.

НЕ ДЕЛАЙТЕ ТАК

JIRA

Evgeny Chentsov

Dashboards | Projects | Issues | Filters | Configure | Reports | Checklists | Send Mail | + Create Issue | Quick Search

A1 / ALLODS-228228

Сделать серверную защиту от спидхака

Edit | Comment | Log Work | Copy Create | More Actions | Decline | Resolve | Reassign | Report duplicate | Workflow | Share | Views

Details

Type: Task

Status: Assigned (View Workflow)

Resolution: Unresolved

Labels: None

Feature Priority:

Feature and Goal: ALLODS Защиты от взломов

Task Severity: Normal

Copy to clipboard: Issue info | Commit info

Description

Сделать чтобы работало идеально.

Activity

All | Comments | Work Log | History | Activity | Transitions | Git Commits | Subversion+

Evgeny Chentsov added a comment - 09.10.2020 20:42

Готово, пусть теперь куа все максимально тщательно тестят.

Comment

People

Assignee: Evgeny Chentsov

Vote (0) | Watching (2)

Time Tracking

Evgeny Chentsov

Original Estimate:	80h
Current Estimate:	80h
Worked:	1180h
Remaining:	0h

ЕВГЕНИЙ ЧЕНЦОВ

программист

e.chentsov@corp.mail.ru

ЕВГЕНИЙ КРУТСКИХ

старший QA-специалист

e.krutskikh@corp.mail.ru

СПАСИБО!