Sécurisation des jeux vidéo – Solutions anti-cheat

Analyse des dispositifs technologiques contre la triche

DESMAZEAUX SAMY

14/02/2025

Problématique :

Quels dispositifs technologiques peuvent être mis en œuvre pour sécuriser un jeu vidéo et prévenir efficacement la création et l'utilisation de cheats ?

Démarche de veille Pour assurer une veille efficace sur le sujet des dispositifs anti-cheat dans les jeux vidéo, plusieurs outils ont été mis en place :

- **Google Alerts : Suivi des articles publiés en ligne sur les thèmes de l'anti-cheat, des mesures de sécurité et des problèmes de triche dans les jeux vidéo.**
- **Reddit & Forums de jeux vidéo : Surveillance des discussions sur les problèmes de triche et les solutions mises en place par les développeurs.**
- **Publications officielles des éditeurs : Suivi des communiqués de presse d'Ubisoft, EA, Valve et autres studios touchés par le problème.**
- **Réseaux sociaux (Twitter, Discord, YouTube) : Consultation des retours des joueurs et des vidéos exposant des cas de triche.**
- **Articles spécialisés et rapports techniques : Études sur les tendances de la triche et sur l'évolution des systèmes anti-cheat.**

Un suivi chronologique a été effectué pour observer l'évolution des problèmes et des solutions mises en place :

- **04/2020 : Annonce de la sortie officielle de *Valorant* et déploiement de *Vanguard* par Riot Games.**
- **06/2020 : Lancement officiel du jeu avec un système anti-triche intégré.**
- **01/10/2024 : Plus de 3,6 millions de tricheurs bannis.**

Analyse argumentée

Exemple de cas d'échec :

L'article du site La Crème du Gaming annonce la perte de plusieurs milliards de dollars en bourse de la part de l'éditeur de jeux Electronic Arts. Cette chute en bourse découle de plusieurs facteurs, mais principalement de la perte de revenus de leur jeu phare, FC25. En effet, le jeu de simulation de football est en perte de vitesse, et l'une des raisons est l'échec d'EA à trouver une solution efficace contre les tricheurs. Pire encore, l'arrivée du Cross-Platform a permis aux tricheurs sur PC, qui détérioraient l'expérience des joueurs sur des modes compétitifs, de se propager sur les joueurs consoles.

Cet exemple est frappant il démontre que lorsque les solutions anti-triche mises en place par les éditeurs de jeux vidéo ne sont pas suffisantes, les conséquences peuvent être désastreuses. En effet, l'impact de la triche dans un jeu en ligne va bien au-delà de l'expérience des joueurs, affectant directement la réputation et les revenus de l'éditeur.

Lorsque des tricheurs parviennent à contourner les mécanismes de sécurité, cela crée une perception négative parmi la communauté de joueurs. Ceux-ci vont avoir le sentiment que le jeu est de mauvaise qualité, ce qui peut entraîner une perte de joueurs actifs, des critiques négatives et une diminution de l'engagement. Le bouche-à-oreille et les évaluations sur les plateformes de téléchargement peuvent également affecter la popularité du jeu, réduisant ainsi les ventes et les microtransactions.

Par ailleurs, l'image de marque d'un éditeur peut être gravement ternie. Dans un marché de plus en plus concurrentiel, où les joueurs sont très exigeants en matière d'équité et d'expérience, les éditeurs doivent investir dans des solutions anti-triche de plus en plus sophistiquées. Cela inclut des systèmes de détection en temps réel, des mises à jour fréquentes pour contrer les nouvelles méthodes de triche et une communication transparente avec la communauté.

À long terme, l'absence d'efforts pour lutter efficacement contre la triche pourrait même nuire à la pérennité de l'entreprise. En plus de la diminution des revenus immédiats, cela pourrait compromettre la fidélité des joueurs et nuire à l'attractivité des futurs projets de l'éditeur, créant un cercle vicieux difficile à rompre. On verra des outils personnalisés fournis par des entreprises externes qui permettent de réduire les coûts pour les éditeurs de jeu.

1. **Les types de triche les plus courants**

Aimbots : Logiciels qui permettent aux joueurs de viser automatiquement et de suivre leurs adversaires dans les FPS, cela peut être paramétré pour en plus suivre l'adversaire et de choisir au préalable la zone de l'adversaire visé.

Wallhacks : Permettent de voir les ennemis à travers les murs, très gros avantage de plus que sur certains jeux les joueurs ont la possibilité de tirer à travers les murs.

Macros et scripts : Automatisent des actions complexes (ex. tir rapide, gestion du recul des armes).

Exploitation de failles : Exploitation de bugs pour obtenir un avantage injuste.

Attaques DDoS : Saturation des serveurs pour provoquer des déconnexions.

Périphériques de triche : Claviers et souris non autorisés sur certaines plateformes. Cronus qui permet d'implémenter des logiciels de triche comme des macros, qui étaient difficile à mettre en place sur console.

2. **Les solutions mises en place par les éditeurs**

Détection automatique des cheats

***BattlEye* : Fonctionne en scannant la mémoire du jeu et du système à la recherche de programmes injectant du code malveillant.**

Analyse les processus en arrière-plan et détecte les signatures de logiciels de triche.

Utilise une liste noire de logiciels connus pour ajuster les détections.

***Easy Anti-Cheat (EAC)* :**

Surveille en temps réel les interactions du joueur avec le jeu.

Détecte les injections de code et les modifications non autorisées des fichiers de jeu.

Utilise un driver au niveau utilisateur pour surveiller les activités suspectes.

***Riot Vanguard* :**

Fonctionne en mode kernel (niveau le plus bas du système d'exploitation) pour surveiller l'ensemble du système dès son démarrage et permet d'accéder au matériel et ressource critique de l'ordinateur comme le processeur.

***Machine Learning* : Analyse des comportements anormaux des joueurs.**

***Vérification de l'intégrité des fichiers* : Comparaison des checksums des fichiers de jeu. Les Checksums sont des valeurs numériques qui vont permettre de vérifier l'intégrité des fichiers, n'importe quel modification même minime sera automatiquement détecté.**

Implication des joueurs :

Possibilité pour les joueurs de signaler un comportement suspect de la part d'u autre joueur pendant le jeu.

CS :GO a mis en place des outils de rediffusion des parties de joueur signalé comme suspecte. Ces rediffusions sont disponibles à tous les joueurs et peuvent en regardant la partie déterminer selon eux si le joueur suspect a effectivement triché ou non.

Machine Learning et analyse comportementale :

Analyse les mouvements des joueurs et détecte des anomalies dans leur comportement.

Implémentation via des algorithmes de détection d'anomalies comme Isolation Forest ou Random Cut Forest.

Ce sont deux systèmes de vérification de données par isolation en comparant avec la moyenne de ce même type de donnée.

Exemples : un taux de précision trop élevé, une réactivité anormale ou des patterns de déplacement non humains.

Sanctions et mesures punitives

Bannissements temporaires ou définitifs, pour les joueurs qui trichent ou les joueurs qui bénéficient de la triche de leur coéquipier de manière trop récurrente

Shadow banning **: Isolation des tricheurs sur des serveurs spécifiques, les joueurs problématiques se retrouvent entre eux et n'ont donc plus d'intérêt de tricher.**

Augmentation de la latence pour les utilisateurs détectés avec des périphériques interdits.

Systèmes de scoring basés sur l'historique de fair-play des joueurs.

Expérimentation de la solution technologique :

L'intégration de l'intelligence artificielle dans la détection de triche commence à montrer des résultats prometteurs. Par exemple, Riot Games a mis en place des algorithmes de machine learning capables de repérer les comportements suspects en analysant les données des joueurs en temps réel. Cette technologie permet non seulement de détecter les tricheurs, mais aussi d'adapter les paramètres de détection pour éviter les faux positifs.

Recommandations

1. **Renforcement de la surveillance préventive**

   Implémentation de systèmes anti-triche dès la phase de développement du jeu.

   Collaboration avec des entreprises spécialisées pour bénéficier des dernières avancées.

2. **Amélioration de la transparence avec la communauté**

   Communiquer régulièrement sur les efforts fournis pour lutter contre la triche.

   Mettre en place un système de signalement plus efficace.

3. **Mise en place de sanctions plus dissuasives**

   Application de pénalités progressives allant de la suspension temporaire à l'interdiction permanente.

   Augmentation des difficultés pour récidiver (ex. vérifications renforcées à la création d'un compte).

Glossaire :

- **Aimbot : Programme permettant de viser automatiquement les adversaires.**
- **Wallhack : Technique qui permet de voir à travers les murs.**
- **Machine Learning : Intelligence artificielle capable d'apprendre et de détecter des comportements suspects.**
- **Shadow banning : Mise à l'écart des tricheurs sur des serveurs spécifiques sans qu'ils le sachent.**
- **FPS : Pour *First Person Shooter*, en français : Tir à la première personne. Pour les jeux de tir à la première personne**

Sources

- **La Crème du gaming : https://www.lacremedugaming.fr/editeur/electronic-arts/ea-games-enregistre-une-perte-de-6-milliards-de-dollars-suite-a-lechec-de-son-projet-phare-191944.html#:~:text=Le%20g%C3%A9ant%20du%20jeu%20vid%C3%A9o,%C3%A0%206%20milliards%20de%20dollars.**
- **Begeek : https://www.begeek.fr/les-jeux-avec-les-systemes-anti-triche-les-plus-efficaces-406221**
- **Ubisoft – Documentation officielle sur l'anti-triche de *Rainbow Six Siege***
- **Riot Games – Fonctionnement de *Riot Vanguard***
- **Valve – Guide sur *Overwatch* et la détection de triche**
- **Activision – Explication du système *Ricochet* sur *Call of Duty***
- **Articles spécialisés de Gamasutra, PC Gamer et Ars Technica**