Yazılım Dünyasında Oyunların Lisanslanması: Yöntemler, Teknolojiler ve Güncel Yaklaşımlar

Licensing of Games in the Software World: Methods, Technologies and Current Approaches

Furkan Akgün

Doç. Dr. Burkay Genç
Tez Danışmanı

Hacettepe Üniversitesi

Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğinin

Bilgisayar Grafikleri Anabilim Dalı için Öngördüğü

Dönem Projesi olarak hazırlanmıştır.

2025

YAYINLANMA FİKRİ MÜLKİYET HAKKLARI BEYANI

Enstitü tarafından onaylanan lisansüstü tezimin/raporumun tamamını veya herhangi bir kısmını, basılı (kağıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Hacettepe üniversitesine verdiğimi bildiririm. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, dönem projemin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları bana ait olacaktır.

Dönem projemin kendi orjinal çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve dönem projemin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Araştırma yazımda yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanması zorunlu metinlerin yazılı izin alarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

..... / ..... /.....

Furkan Akgün

ÖZET

Oyun sektörü, dijital teknolojilerin gelişimiyle birlikte en hızlı büyüyen endüstrilerden biri haline gelmiştir. Bu büyümeyle birlikte korsan yazılım kullanımı da artmış ve yazılım lisanslama teknolojilerinin önemi daha da belirginleşmiştir. Bu araştırma yazısı, oyun dünyasında kullanılan lisanslama yöntemlerini tarihsel süreç içerisinde ele alarak, günümüzde yaygın olarak tercih edilen çözümleri karşılaştırmalı olarak incelemektedir.

Çalışmada ilk olarak yazılım lisanslamasının temel kavramları açıklanmış, ardından 1980'lerden günümüze oyun lisanslamasının geçirdiği evrim detaylandırılmıştır. 1990'lı yıllardaki donanım tabanlı çözümlerden 2000'li yıllardaki dijital dağıtım devrimine, 2010 sonrası gelişmiş DRM teknolojilerinden günümüzün bulut ve blokzincir tabanlı sistemlerine kadar çok sayıda yöntem değerlendirilmiştir.

Araştırmada Denuvo, CodeMeter, Steamworks, Epic Online Services ve VMProtect gibi güncel lisanslama teknolojileri; güvenlik, performans, maliyet ve kullanıcı deneyimi kriterleri doğrultusunda karşılaştırılmıştır. Ayrıca, yeni nesil lisanslama trendleri arasında yer alan NFT tabanlı lisanslar, Game-as-a-Service modeli ve yapay zekâ destekli lisans izleme gibi yaklaşımlar analiz edilmiştir.

Bu çalışmanın temel amacı, oyun geliştiricilere lisanslama stratejilerini belirlemede kapsamlı ve analitik bir yol haritası sunmak; aynı zamanda korsan yazılım ile mücadelede kullanıcı dostu ve sürdürülebilir yöntemleri vurgulamaktır.

ABSTRACT

The video game industry has emerged as one of the fastest-growing digital sectors, fueled by rapid technological advancements and global market expansion. Alongside this growth, the prevalence of software piracy has increased significantly, highlighting the critical role of licensing technologies. This research paper examines software licensing systems used in the gaming world, analyzing their historical development and comparing contemporary solutions in terms of efficiency, security, and user experience.

The study begins with the fundamental concepts of software licensing and continues with a chronological overview of game licensing practices from the 1980s to the present. It explores the transition from hardware-based dongles in the 1990s to the rise of online distribution and activation in the 2000s, and the widespread use of advanced DRM technologies like Denuvo and CodeMeter in the 2010s. Current trends such as cloud-based and blockchain-powered licensing models are also evaluated.

Contemporary licensing tools—including Denuvo, CodeMeter, Steamworks, Epic Online Services, and VMProtect—are analyzed across multiple criteria such as security level, system performance, integration ease, and cost. The study also explores emerging approaches like NFT-based licensing, Game-as-a-Service (GaaS) models, and AI-driven license behavior tracking.

The primary objective of this research is to offer game developers a structured and comprehensive guide for selecting appropriate licensing strategies while emphasizing the balance between anti-piracy effectiveness and player satisfaction.

İÇİNDEKİLER

1. Giriş

Yazılım, günümüz dijital dünyasında bireylerin ve işletmelerin yaşamlarını doğrudan etkileyen temel bileşenlerden biridir. Bilgi teknolojilerinin hızla gelişmesiyle birlikte, yazılımların korunması ve izinsiz kullanımlarının engellenmesi önem kazanmıştır. Özellikle oyun endüstrisi gibi yoğun rekabetin bulunduğu, hızlı tüketimin yaşandığı ve korsan kullanımın sıkça görüldüğü alanlarda yazılım lisanslaması daha da kritik hale gelmiştir.

Oyun sektöründe, yazılım ürünlerinin yetkisiz kopyalanmasının ve dağıtımının önlenmesi, geliştiricilerin ekonomik çıkarlarını korumak için hayati önem taşımaktadır. Ayrıca lisanslama yöntemlerinin, kullanıcı deneyimini olumsuz etkilemeden ve oyun performansını düşürmeden uygulanması gerekmektedir. Bu durum, lisanslama teknolojilerini ve yöntemlerini karmaşık hale getirerek sektörün önemli teknik zorluklarından biri olmuştur.

Bu araştırmanın amacı, oyun sektöründe kullanılan lisanslama yöntemlerini ve teknolojilerini kapsamlı biçimde inceleyerek, tarihsel gelişim süreci içinde değerlendirmek ve günümüzde en sık kullanılan lisanslama ürünlerini detaylı olarak analiz etmektir. Ayrıca gelecekteki eğilimleri ve yenilikçi çözümleri de ele alarak oyun geliştiricilerine ve sektör paydaşlarına stratejik öneriler sunmak hedeflenmektedir.

Araştırma kapsamında, öncelikle yazılım lisanslamasına dair temel kavramlar ve oyun sektöründeki özgün ihtiyaçlar anlatılacak, ardından lisanslama teknolojilerinin kronolojik ve teknik gelişimi incelenecektir. Daha sonra güncel lisanslama çözümlerinin teknik ve ekonomik analizleri gerçekleştirilerek, karşılaştırmalı bir değerlendirme yapılacaktır. Son olarak ise gelecekte sektörü şekillendirecek yeni nesil yaklaşımlar ve öneriler sunulacaktır.

Bu çalışmanın sonuçlarının, hem akademik olarak oyun yazılımlarının korunmasına ilişkin literatüre katkı sağlaması hem de oyun geliştiricilerinin lisanslama stratejileri geliştirmesine rehberlik etmesi beklenmektedir.

2. GENEL BİLGİLER

Yazılım ürünlerinin kullanımı ve dağıtımına yönelik izinleri düzenleyen süreçlere genel anlamda yazılım lisanslaması denir. Yazılım lisanslaması, geliştiricilerin ve yayıncıların yazılımlar üzerindeki haklarını korurken, kullanıcıların da yazılımları hangi koşullarda kullanabileceklerini net olarak tanımlar.

2.1. Yazılım Lisanslamasına Genel Bakış

Yazılım lisanslama, genel olarak bir yazılım ürününün kullanım haklarının geliştirici veya yayıncı tarafından belirli koşullara bağlanarak kullanıcıya sunulmasıdır. Lisanslama yöntemleri genellikle şu hedeflerle uygulanır:

- Ürünün yasa dışı kopyalanmasını ve dağıtılmasını önlemek,
- Yazılımın kullanım koşullarını net olarak tanımlamak,
- Geliştirici ve kullanıcı arasındaki yasal sorumlulukları belirlemek.

Yazılım lisansları farklı kullanım türlerine ve yazılımın dağıtım şekline göre sınıflandırılır. Temel lisans türleri aşağıda özetlenmiştir:

Açık Kaynak Lisansları (Open-Source): Bu lisans türü, yazılımın kaynak kodunun kullanıcılar tarafından serbestçe erişilebilir ve değiştirilebilir olmasına izin verir. Popüler açık kaynak lisansları şunlardır:

- MIT Lisansı
- GNU GPL (General Public License)
- Apache Lisansı

Bu lisanslar genellikle topluluk tabanlı projelerde yaygın olarak tercih edilir ve kullanıcıların yazılımı özgürce kullanmasını, değiştirmesini ve dağıtılmasını sağlar.

Ücretsiz ve Ücretli Lisanslar (Freeware, Commercial)

- Ücretsiz (Freeware): Kullanıcıya ücretsiz olarak dağıtılan fakat kaynak kodu genellikle erişime kapalı olan yazılımlardır.
- Ücretli (Commercial): Kullanıcıların belirli bir ücret karşılığında satın aldığı, genellikle profesyonel destek ve güncellemelerle birlikte sunulan yazılımlardır.

Abonelik Tabanlı Lisanslar (Subscription-based Licensing): Belirli sürelerle yenilenen kullanım hakkı sağlayan lisanslama türüdür. Kullanıcılar genellikle aylık ya da yıllık ücretler ödeyerek yazılıma erişir. Bu yöntem özellikle bulut tabanlı yazılımlar ve servis olarak yazılım (Software as a Service - SaaS) uygulamaları için tercih edilir.

2.2. Oyun Sektöründe Lisanslama

Oyun sektörü, yazılım lisanslamasının en kritik olduğu alanlardan biridir. Bu sektörde lisanslamanın temel hedefleri şunlardır:

- Korsan Yazılım Sorunu ile Mücadele:
  Oyunlar genellikle yüksek maliyetlerle geliştirilen ürünlerdir ve korsan kullanım, oyun geliştiricileri için ciddi ekonomik kayıplara yol açmaktadır. Oyunlarda lisanslama çözümleri bu nedenle korsan kullanımın önüne geçecek güçlü yöntemlere ihtiyaç duyar.

- Kullanıcı Deneyimini Korumak:
  Oyun lisanslama çözümlerinin oyuncuların deneyimini olumsuz etkilememesi gerekir. Oyuncuların lisanslama süreçleri nedeniyle yaşadığı zorluklar (örneğin sürekli online bağlantı gerekliliği, performans düşüşleri vb.) oyunun başarısını doğrudan etkileyebilir.

- Performans Dengesini Sağlamak:
  DRM ve diğer lisanslama sistemleri, oyunların performansına ek yük getirebilir. Bu nedenle, oyun geliştiricileri lisanslama yöntemlerini seçerken performans maliyetlerini dikkatlice değerlendirmelidir.

- Crack ve Bypass Yöntemlerine Karşı Direnç:
  Popüler oyunlar için çok kısa sürelerde crack yazılımları piyasaya sürülebilmekte ve lisanslama yöntemleri devre dışı bırakılabilmektedir. Gelişmiş ve sürekli güncellenen lisanslama çözümlerine olan ihtiyaç bu nedenle sürekli artmaktadır.

Oyun sektöründe lisanslama, klasik seri numarası dağıtımından bulut tabanlı ileri DRM çözümlerine kadar geniş bir yelpazede yer alır. Günümüzde özellikle CodeMeter, Denuvo gibi teknolojiler, yüksek güvenlik seviyesi ve performans dengesi nedeniyle popüler hale gelmiştir.

Bu bölümde verilen bilgiler ışığında, bir sonraki bölümde lisanslama yöntemleri ve teknolojileri detaylandırılarak oyun lisanslamasındaki tarihsel gelişim incelenecektir.

3. LİSANSLAMA YÖNTEMLERİ VE TEKNOLOJİLERİ

Yazılım lisanslama yöntemleri, yazılımın kullanımını kontrol etmek, yetkisiz dağıtımını önlemek ve yazılım geliştiricilerinin ticari haklarını korumak amacıyla oluşturulmuştur.

3.1. Geleneksel Lisanslama Yöntemleri

Seri Numarası ve Aktivasyon Kodları

Bu yöntem, bir yazılım ürünü satın alındığında kullanıcıya benzersiz bir seri numarası veya aktivasyon kodu verilmesine dayanır. Bu kod yazılımın ilk kurulumu sırasında istenir ve doğrulandıktan sonra yazılım kullanıma açılır. Bu yöntem özellikle oyun sektörünün erken dönemlerinde sıklıkla kullanılmıştır.

Electronic Arts (EA**)** tarafından geliştirilen erken dönem oyunlarda (örneğin FIFA serisinin eski sürümleri), kutulu oyunların içinde benzersiz seri numaraları bulunur ve kullanıcılar bu kodları girerek oyunlarını etkinleştirirdi.

Avantaj olarak basit ve düşük maliyetli bir çözüm olduğu söylenebilir. Ayrıca hızlı ve kullanıcı dostudur.

Dezavantajlar ise seri numaraları paylaşılabilir veya crack yazılımlarıyla kolayca aşılabilir.Çok sınırlı güvenlik sağlar.

Donanım Tabanlı Lisanslama (Dongle, USB Anahtarlar)

Bu yöntem, yazılımın kullanımı için fiziksel bir cihazın (dongle) bilgisayara takılı olması zorunluluğuna dayanır. Yazılım, bu fiziksel donanımı doğrulayarak çalışır.

Yazılım sektöründe, özellikle profesyonel CAD yazılımları (Autodesk ürünleri gibi) uzun süre USB dongle'ları kullanmıştır. Oyun sektöründe daha az tercih edilmiştir ancak Arcade oyun makinelerinde fiziksel anahtarlar sıklıkla görülmüştür.

Avantajı ise güvenliği çok yüksek olmasıdır. fiziksel cihaz olmadan yazılımı çalıştırmak zordur.

Dezavantajları ise yüksek maliyetlidir ve kullanıcıya ek bir yük getirir (dongle kaybı, fiziksel hasar riski) ve kullanıcı deneyimini olumsuz etkileyebilir.

3.2. Dijital Haklar Yönetimi (DRM - Digital Rights Management)

DRM, dijital içeriklerin (oyun, müzik, film vs.) dağıtımını ve kullanımını yönetmek amacıyla geliştirilmiş ileri düzey koruma teknolojisidir. Oyun sektöründe DRM sistemleri, yazılımın crack ve korsan versiyonlarından korunmasını amaçlar.

DRM sistemlerinin sağladığı temel özellikler ise şöyle örnek verilebilir: Yazılım kodunun şifrelenmesi ve runtime kontrolleri. Online veya periyodik lisans doğrulama.Kullanıcıların yazılıma erişiminin çeşitli şartlarla sınırlandırılması (süre sınırlaması, cihaz sınırlaması vs.).

3.3. Online Aktivasyon ve Bulut Tabanlı Lisanslama

Online Aktivasyon

Online aktivasyon yöntemi, internet üzerinden merkezi bir aktivasyon sunucusuyla doğrulama yapılarak çalışır. Kullanıcı satın aldığı oyunu ilk kez çalıştırdığında sunucudan lisans onayı alır.

Valve'ın **Steam** platformu bu yöntemi yaygınlaştırmıştır. Kullanıcılar oyunu satın aldıklarında Steam üzerinden otomatik olarak online aktivasyon gerçekleşir. Korsan kullanımın önüne geçmede çok etkilidir ve merkezi lisans yönetimi sağlar.İnternet bağlantısı gereklidir; bağlantı sorunlarında kullanıcı erişimi kısıtlanabilir.

Bulut Tabanlı Lisanslama

Yazılımın lisansının ve kullanımının tamamen bulut tabanlı sistemler üzerinden yönetilmesi anlamına gelir. Lisans bilgisi sürekli olarak çevrimiçi doğrulama ile kontrol edilir.

Ubisoft şirketinin geliştirdiği Uplay (Ubisoft Connect), bulut tabanlı lisanslama yöntemini kullanır. Assassin's Creed serisi gibi popüler oyunlarda bu yöntem kullanılır.

Avantajı çok yüksek güvenlik düzeyi sunmasıdır ayrıca.Lisans yönetimini ve kullanım takibini kolaylaştırır.

Dezavantajları ise sürekli internet bağlantısı gerektirir ve sunucu sorunları kullanıcıları etkileyebilir.

3.4. Güncel DRM ve Güvenlik Çözümleri (Denuvo, CodeMeter ve VMProtect)

Denuvo Anti-Tamper Teknolojisi

Denuvo, son yılların en popüler DRM çözümüdür. Yazılımın kodunu gerçek zamanlı olarak şifreleyip, yazılımın çalışma mantığını saklayarak crack işlemlerini zorlaştırır.

FIFA serisi (EA Sports), Doom Eternal (Bethesda), Resident Evil serisi (Capcom) gibi oyunlar aktif olarak kullanmaktadır.

CodeMeter Lisanslama Sistemi

CodeMeter, lisanslama ve DRM koruma özelliklerini donanım ve yazılım tabanlı seçeneklerle sağlayan çok yönlü bir çözümdür. Kullanıcı dostu arayüzü ile geliştiricilere lisanslama sürecini kolaylaştırır.

Oyun sektöründe kullanımı sınırlıdır, genellikle endüstriyel ve profesyonel yazılımlarda kullanılır**.** Ancak profesyonel simülasyon oyunları ve eğitsel oyunlarda tercih edilebilir.

VMProtect (Kod Obfuscation)

VMProtect, yazılımın kodunu sanal bir makinede çalıştırarak ve kodu karmaşıklaştırarak (obfuscation) crack edilmesini ciddi oranda zorlaştıran bir güvenlik çözümüdür.

Oyun geliştiricileri tarafından doğrudan değil, Denuvo gibi diğer DRM sistemleri ile birlikte kullanılır. Bu durum, oyun crack süreçlerini ciddi biçimde geciktirebilir.

4. OYUN LİSANSLAMASINDA KRONOLOJİK GELİŞİM VE TEKNİK ANALİZ

Oyun sektöründe yazılım lisanslaması, bilgisayar teknolojilerindeki gelişmeler, kullanıcı talepleri ve korsan yazılımın sektörde oluşturduğu ciddi ekonomik baskılar doğrultusunda sürekli olarak evrim geçirmiştir. Bu bölümde, oyun firmalarının bu süreçte karşılaştığı önemli zorluklar, geliştirdikleri çözümler ve sektörün bu çözümlere verdiği tepkiler kronolojik bir bakış açısıyla derinlemesine incelenmiştir. Bu bölümde ayrıca oyunların korunması için geliştirilen teknolojilerin teknik yapısı ve korsanların bu yazılımları ve teknolojileri nasıl aştığı detaylı olarak incelenmiştir.

4.1. 1980’ler – Basit Seri Numaraları ve Manuel Aktivasyon Dönemi

1980’li yıllar, kişisel bilgisayarların ilk kez geniş kullanıcı kitlesine ulaştığı, evlerde bilgisayar kullanımının arttığı ve oyun sektörünün hızla büyüdüğü önemli bir dönemi işaret eder. Bu büyüme dönemi, oyun geliştiricileri açısından hem yeni fırsatlar hem de önemli zorlukları beraberinde getirdi. Bu dönemde oyun endüstrisinin karşılaştığı en büyük sorunlardan biri, oyunların izinsiz kopyalarının kolayca oluşturulması ve dağıtılmasıydı.

Oyun firmaları, yazılımlarının yetkisiz kopyalarının yapılmasını engellemekte ciddi güçlük çekti. Bu durum, satışların düşmesine, oyunların orijinal kopyalarının değerinin azalmasına ve oyun geliştiricilerinin büyük ekonomik zararlara uğramasına neden oldu. Özellikle disketlerin kolayca kopyalanabilir olması, korsan kullanımın önünü açan en temel faktördü.

Bu soruna çözüm olarak oyun geliştiricileri, kutu oyunlarıyla birlikte basılı olarak sunulan ve kullanıcıların oyunlarını yüklerken manuel olarak girmeleri gereken basit seri numaraları ve

aktivasyon kodlarını kullanmaya başladılar. Bu yöntem, temel olarak kutunun içinde basılı bir belge olarak bulunan benzersiz bir numara veya kombinasyon içeriyordu. Kullanıcılar bu numaraları yazılımı kurarken doğru bir şekilde girerek oyunu aktive edebiliyorlardı.

Örneğin, Commodore 64, ZX Spectrum ve Atari gibi popüler platformlarda piyasaya sürülen oyunlar genellikle kutu içeriğinde bulunan seri numarası veya basılı kod kılavuzlarıyla korunmaktaydı. Bu kodlar, genellikle oyunların yükleme ekranlarında ya da kurulum aşamasında kullanıcıdan isteniyordu.

Ancak, bu sistemin ciddi zayıflıkları vardı. İlk olarak, seri numaraları ve aktivasyon kodları, kullanıcılar arasında kolayca paylaşılabilir durumdaydı. Bir kullanıcı tarafından elde edilen bir kod, diğer kullanıcılar tarafından rahatlıkla yeniden kullanılabiliyor ve böylece oyun korsanlığının önüne geçmek mümkün olmuyordu.

İkinci olarak, bu manuel sistem kullanıcı açısından büyük zahmetler yaratıyordu. Kullanıcılar kutularını veya içindeki belgeleri kaybettiklerinde, oyunlarını kurmak veya yeniden yüklemek için ciddi sorunlar yaşayabiliyorlardı. Bu durum kullanıcı memnuniyetini azaltıyor ve oyun firmaları için olumsuz müşteri deneyimi yaratıyordu.

1980’li yılların sonunda özellikle Sierra On-Line, LucasArts gibi firmaların ürettiği popüler macera oyunları (örneğin King's Quest, Monkey Island serileri), daha karmaşık bir yöntem olan "kod tabloları" ya da "fiziksel koruma yöntemleri" kullanmaya başladılar. Oyunun belirli bir noktasında kullanıcıdan kılavuzdaki belirli bir sayfadan veya görselden alınan özel bir kelime ya da sembol girilmesi isteniyordu. Kullanıcı kılavuza veya kutu içindeki fiziksel materyale sahip olmadan bu adımı geçemiyordu. Bu, fiziksel materyale sahip olmayan korsan kopya kullanıcılarının oyunları oynamalarını zorlaştıran yaratıcı bir yöntemdi.Örneğin bu kod tabloları oldukça koyu arka planlı hafif silik bir şekilde yazılı bir şekilde geliyordu. Bu kağıdı yazıcı ile kopyalamaya çalışırsanız sadece siyah bir baskı elinize geçiyordu. Böylece kopyalamayı zorlaştırma hedeflenmişti.Örneğin, LucasArts tarafından piyasaya sürülen "The Secret of Monkey Island" oyununda oyuncular, kutudaki özel dönen disk (code wheel) üzerinden eşleşen sembolleri bulmak zorundaydılar. Bu koruma yöntemi kullanıcıların fiziksel kopyaları saklamalarını teşvik ediyor ve korsan kullanımı önemli ölçüde azaltıyordu. Ayrıca bu dönemde bulunan ünlü lenslokta yaratıcı bir çözümdü. 1980’lerde oyun korsanlığını önlemek amacıyla geliştirilen Lenslok, özellikle TT Racer ve Tomahawk gibi popüler oyunlarda kullanılan ilginç ama tartışmalı bir kopya koruma yöntemiydi. Küçük bir plastik prizma olan bu cihaz, oyun başlatıldığında ekrana yansıtılan bozulmuş bir kodu yalnızca belirli bir mesafeden ve açıdan bakıldığında okunabilir hale getiriyor, oyuncudan bu kodu doğru şekilde girerek oyunu başlatmasını istiyordu. Özellikle TT Racer’ın geniş oyuncu kitlesi, Lenslok’un neden olduğu erişim sorunlarını sıkça gündeme getirirken, Tomahawk gibi daha simülasyon odaklı yapımlar ise zaten karmaşık oynanışa sahipken bu ek fiziksel bariyerle kullanıcı deneyimini daha da zorlaştırdı. Cihazın ekran boyutuna duyarlı olması, çoğu kullanıcının doğru mesafeyi tutturamaması ve kullanım kılavuzlarının yetersizliği nedeniyle Lenslok, yaratıcı bir fikir olmasına rağmen pratikte büyük hayal kırıklığı yarattı. Yazılım tabanlı koruma yöntemlerinin gelişmesiyle hızla tarihe karışan bu sistem, korsanla

mücadelede donanım temelli çözümlerin ne kadar kullanıcı dostu olması gerektiğine dair önemli bir örnek olarak anılmaktadır.

Aslında lenslok bir nevi 1980'lerin iki faktörlü doğrulama sistemi gibi düşünülebilir: Yazılım + fiziksel cihaz olmadan çalışmıyordu. Ancak kullanıcı deneyimini ikinci plana atması onu tarihte kötü bir örnek haline getirdi.

Son olarak dönemin bir oyunu copy protection alanındaki başarısıyla ön plana çıkıyordu. Dungeon Master (1987), bu oyun yalnızca yenilikçi oynanışıyla değil, aynı zamanda dönemin en gelişmiş kopya koruma yöntemlerinden birini kullanmasıyla da dikkat çeken bir oyun olmuştur. Geliştirici FTL Games, korsan kopyaların yayılmasını önlemek için standart dışı bir disk formatı kullanarak oyun disketini özel bir yapıda tasarlamıştır. Bu yapı, dönemin popüler kopyalama yazılımlarının oyunu çoğaltmasını engellemişti, çünkü bu yazılımlar yalnızca standart disk yapılarıyla çalışabilmekteydi. Ayrıca diskin bazı bölgelerine bilinçli olarak bozuk sektörler eklenmiş, oyun bu hataları orijinallik kontrolü için kullanmıştır. Yazılım, disk kontrolünü işletim sisteminden bağımsız olarak doğrudan donanım düzeyinde gerçekleştirdiğinden, bu kontroller çoğu zaman atlatılamamıştır. Sadece oyunun başlangıcında değil, oyun ilerledikçe de yapılan bu çok katmanlı kontroller sayesinde, kopyalanmış sürümler çoğunlukla çalışmamış ya da oyun sonuna ulaşılamamıştır. Bunun yanı sıra oyunun fiziksel materyalleri (manuel, harita, sihirli alfabe gibi) da oynanış için gerekli olduğundan, bu belgeler olmadan ilerlemek mümkün değildi. Dungeon Master'ın bu sofistike koruma yöntemleri, onu 1980'lerin en zor kopyalanabilen ve bu yönüyle en başarılı koruma sistemine sahip oyunlarından biri haline getirmiştir.

Bu Dönemin Avantajları ve Dezavantajları

Avantajları:

- Kullanımı basit ve ucuz maliyetliydi.
- Oyunları ilk kez satın alan kullanıcılara lisanslama bilinci oluşturulmaya başlandı.

Dezavantajları:

- Kullanıcı deneyimi açısından zorlayıcıydı ve zaman zaman büyük kullanıcı rahatsızlıklarına yol açıyordu.
- Korsan kopyalamayı tamamen engellemede yetersiz kalıyordu.
- Seri numaralarının ve koruma materyallerinin kaybolması kullanıcılar için ciddi sorun oluşturabiliyordu.

1980'lerin lisanslama yöntemleri, oyun sektörünün gelecekte karşılaşacağı daha karmaşık lisanslama yöntemlerine geçişte temel oluşturmuştur. Bu dönemdeki basit çözümler, korsanlık sorununu ortadan kaldırmamış olsa bile, kullanıcıları yazılımların yasal haklarına saygı duymaya teşvik eden ilk adımlar olarak görülebilir. Aynı zamanda, gelecekteki daha gelişmiş DRM sistemlerine de zemin hazırlayarak oyun sektöründe kullanıcı hakları ve koruma yöntemleri üzerine tartışmaların başlamasına sebep olmuştur.

4.2. 1990’lar – Donanım Tabanlı Koruma ve Disk Bazlı DRM Dönemi

4.2.1. Dongle (Donanım Anahtarı) Tabanlı Koruma Yöntemleri

1980'lerin sonlarından itibaren, yazılım korsanlığını önlemek amacıyla dongle adı verilen donanım anahtarları kullanılmaya başlandı. Bu cihazlar, genellikle bilgisayarın paralel veya seri portuna takılarak yazılımın çalışması için gerekli bir donanım bileşeni haline getirildi.

Dongle'lar, yazılımın belirli aralıklarla bu donanımı kontrol etmesini sağlayarak, donanımın varlığını doğruluyordu. Bu yöntem, özellikle yüksek maliyetli profesyonel yazılımlarda ve bazı oyunlarda tercih edildi.

Avantajları**:**

- Fiziksel bir cihaz olduğundan, yazılımın yetkisiz kopyalanmasını zorlaştırdı.
- Donanım tabanlı olduğu için yazılım korsanlarının aşması daha zordu.

Dezavantajları**:**

- Kullanıcılar için ek bir donanım gereksinimi oluşturdu.
- Dongle'ların kaybolması veya bozulması durumunda yazılım kullanılamaz hale geldi.

1985 yılında ZX Spectrum 48K için geliştirilen "Shadow of the Unicorn" oyunu, Mikro-Gen Ltd tarafından üretilen Mikro-Plus dongle'ı ile birlikte sunuldu. Bu dongle, oyunun çalışması için gerekli olan 16KB'lık ek bir ROM içeriyordu .

4.2.2. SafeDisc: Macrovision'un Disk Bazlı DRM Çözümü

1998 yılında Macrovision Corporation tarafından geliştirilen SafeDisc, CD-ROM'lar için bir kopya koruma programıydı. SafeDisc, orijinal disklerde belirli veri imzaları ve "bad sectors" oluşturarak, bu disklerin kopyalanmasını zorlaştırmayı amaçladı.

SafeDisc, Windows işletim sistemlerinde "secdrv.sys" adlı bir sürücü kullanarak çalışıyordu. Ancak, bu sürücü zamanla güvenlik açıklarına neden oldu. Microsoft, bu güvenlik endişeleri nedeniyle Windows 10 ve sonraki sürümlerde SafeDisc desteğini sonlandırdı.

SafeDisc nasıl çalışıyordu?,SafeDisc aslında oyun çalıştırıldığında CD üzerindeki bu özel imzayı kontrol eder; imza eksikse veya doğru şekilde okunamıyorsa oyun başlatılmaz. Ayrıca, yürütülebilir dosyalar şifrelenerek koruma katmanı güçlendirilmiş, sanal sürücüler veya hata ayıklayıcı programlar tespit edildiğinde oyun çalışması durdurulmuştur. Bu sayede, geleneksel disk kopyalama yazılımlarının SafeDisc korumalı oyunları çoğaltması büyük ölçüde engellenmiştir. Ancak zamanla bu sistem güvenlik açıkları nedeniyle eleştirilmiştir. Bir döneme damgasını vurmuş etkili bir koruma sistemi olarak dijital oyun tarihinde önemli bir yere sahiptir.

SafeDisc, dönemin en karmaşık kopya koruma sistemlerinden biri olmasına rağmen, zaman içinde korsanlar tarafından hem yazılımsal hem de donanımsal düzeyde sistematik biçimde aşılmıştır. Öncelikli hedef, oyunların sadece orijinal diske sahipken çalışmasına izin veren disk doğrulama mekanizması olmuştur. Bu kontrol, yürütülebilir dosya (EXE) içindeki sabit algoritmalarla sağlandığından, tersine mühendislik araçları (örneğin IDA Pro, OllyDbg, SoftICE) kullanılarak analiz edilmiş, ve bu kontrollerin bulunduğu alanlarda küçük binary patching işlemleriyle CD doğrulaması tamamen devre dışı bırakılmıştır. Bir diğer yaygın yöntem ise, SafeDisc'in oyun EXE dosyasını şifreleyerek sarmaladığı yapıyı (wrapper) çözmeye yönelmiştir. Korsanlar, orijinal diskin takılmasıyla belleğe açılan bu şifreli yapıyı RAM üzerinden "dump" ederek, gerçek oyun koduna ulaşmayı başarmış ve ardından PE yapısını (Import Table, Entry Point) yeniden inşa ederek, SafeDisc'den arındırılmış bağımsız çalışabilir sürümler üretmişlerdir. Ayrıca, sistem seviyesinde çalışan SafeDisc sürücüsü secdrv.sys, ya doğrudan kapatılarak ya da sistem yapılandırması değiştirilerek etkisiz hale getirilmiş; bu sayede oyun, diski kontrol eden çekirdek bileşen olmaksızın çalıştırılabilmiştir. Daha ileri düzey korsan yöntemleri arasında, disk üzerinde aranan subchannel ve bozuk sektör verilerini taklit eden gelişmiş sanal sürücü emülatörleri (Daemon Tools, Alcohol 120%) ile koruma atlatılmıştır. SafeDisc'in zamanla geliştirilen sürümleri bu yazılımları tespit edip çalışmayı durdursa da, korsan gruplar sürekli olarak yeni bypass teknikleri ve "No-CD Crack" araçları geliştirerek korumayı aşmayı başarmıştır. Tüm bu süreç, dijital kopya korumanın mutlak olmadığını ve yazılım-donanım uyumunun yanı sıra, sistem davranışlarının gizlenmesinin de kritik önem taşıdığını göstermektedir.

Sonuç olarak SafeDisc, zamanının en sofistike kopya koruma sistemlerinden biri olsa da, korsanlar tarafından hem donanım düzey**i** hem de yazılım seviyesi üzerinden sistematik olarak çözüldü. Reverse engineering tekniklerinin gelişmesi, sistem belleği analiz araçlarının yaygınlaşması ve SafeDisc'in yapısal zayıflıkları nedeniyle, sistem korsanların önünde uzun süre duramadı. Bu da, kopya koruma sistemlerinde donanımsal korumaların tek başına yeterli olmadığını ve yazılımın dinamik davranışlarını gizlemenin önemini gösterdi.

Avantajları**:**

- Disklerin fiziksel özelliklerini kullanarak kopya koruması sağladı.
- Korsan kopyaların çalışmasını engelledi.

Dezavantajları**:**

- Sistem uyumluluk sorunlarına ve performans düşüşlerine neden oldu.
- Güvenlik açıkları oluşturdu ve bazı oyunların çalışmasını engelledi.

"Call of Duty 4", "Age of Empires", "Prince of Persia" ve "Morrowind" gibi popüler oyunlar SafeDisc koruması ile piyasaya sürüldü .

4.2.3. SecuROM: Sony DADC'nin Gelişmiş DRM Sistemi

SecuROM, Sony DADC tarafından özellikle Windows tabanlı bilgisayar oyunlarında lisanslama, kopya koruma ve yetkisiz çoğaltmanın önüne geçmek amacıyla geliştirilen gelişmiş bir dijital hak yönetimi sistemidir. İlk kez 1999 yılında kullanılmaya başlanan bu teknoloji, fiziksel medya temelli kopya koruma yöntemlerinin ötesine geçerek çok katmanlı bir güvenlik mimarisi sunmuştur. SecuROM'un en ayırt edici özelliği, "Data Position Measurement (DPM)" adı verilen yöntemle, orijinal optik diskler üzerinde üretim sırasında oluşturulan fiziksel bozulmaları okuyarak medyanın sahte olup olmadığını yüksek hassasiyetle tespit etmesidir. Bu fiziksel izler, geleneksel CD/DVD yazıcılar tarafından taklit edilemediğinden, korsan kopyalar doğrudan sistem tarafından reddedilir. Yazılım seviyesinde ise, SecuROM şifrelenmiş yürütülebilir dosyaları çalıştırmadan önce yalnızca geçici olarak belleğe çözerek çalıştırmakta ve bu süreçte kodu sadece ihtiyaç anında çözerek anti-debug ve anti-tamper mekanizmalarını devreye sokmaktadır. Sistem, tersine mühendislik araçlarına karşı çeşitli koruma teknikleri (örneğin SEH manipülasyonu, API hook kontrolü, bellek sahası bütünlük testleri) içerir ve sanal sürücü yazılımlarını algılayarak oyunların bu ortamlarda çalışmasını engelleyecek önlemler uygular. 2005 sonrası sürümlerinde eklenen online aktivasyon sistemi sayesinde, lisans anahtarları donanım bileşenlerinden oluşturulan benzersiz bir sistem imzası ile eşleştirilmiş, bu sayede aynı anahtarın birden fazla cihazda kullanımı sınırlanmıştır. Bazı sürümlerde ise sistem sürücüsü (.sys) olarak işletim sistemi seviyesinde çalışan bileşenler ile Virtual File System entegrasyonu sunulmuş, böylece DRM kontrolü daha düşük seviyelerde sağlanmıştır. Tüm bu yönleriyle SecuROM, geleneksel CD kopya koruma çözümlerinden çok daha kapsamlı ve dirençli bir sistem olarak öne çıkmıştır.

Avantajları**:**

- Gelişmiş kopya koruma teknikleri ile korsan kopyaların çalışmasını engelledi.
- Çevrimiçi aktivasyon ile lisans yönetimini kolaylaştırdı.

Dezavantajları**:**

- Kullanıcı deneyimini olumsuz etkiledi ve sistem performansını düşürdü.
- Gizli yazılım yüklemeleri nedeniyle güvenlik ve gizlilik endişelerine yol açtı.

SecuROM Nasıl Aşıldı ?

SecuROM, fiziksel disk doğrulaması, yürütülebilir dosya şifreleme, bellek içi şifre çözme, anti-debug ve anti-emülasyon önlemleri gibi çok katmanlı bir koruma mimarisi sunmasına rağmen, korsan gruplar tarafından zaman içerisinde etkili bir şekilde aşılmıştır. Sistemin ilk katmanı olan Data Position Measurement (DPM) tekniği, optik diskin fiziksel üretim sürecinde oluşturulan özel bozulmaları (örneğin iz genişliği, jitter) okuyarak kopya diskleri tespit etmeye yöneliktir. Ancak gelişmiş optik imaj alma yazılımları (örneğin Alcohol 120%, BlindWrite), bu fiziksel verileri destekleyen özel formatlarla (örneğin .mds, .b5t) disk imajlarını çıkartmış ve gelişmiş sanal sürücü yazılımları (Daemon Tools Pro gibi) aracılığıyla bu imajları orjinal disk gibi sisteme sunmuştur. Ayrıca, diski doğrulayan kodlar tersine

mühendislik araçları kullanılarak bulunmuş ve makine dili düzeyinde işlevsizleştirilerek (NOP talimatlarıyla) geçersiz kılınmıştır.

Yürütülebilir dosyanın şifrelenmiş hâlini çözümleyen loader ise bellekte geçici olarak çözülerek çalıştırılmaktaydı. Bu noktada korsanlar, oyun çalıştıktan sonra RAM dump yöntemi ile çözülmüş kodu elde etmiş; ardından bu kod yeniden derlenerek bağımsız bir "cracked" sürüm oluşturulmuştur. Bu işlem sırasında Import Address Table (IAT) yeniden yapılandırılmış, PE başlığı düzeltilmiş ve oyun dosyası yeniden çalıştırılabilir hâle getirilmiştir. Gelişmiş korumalı sürümlerde ise SecuROM, kodun yalnızca kendi tanımlı sanal makinesi içinde çalışmasına izin veren özel bir sanallaştırma katmanı sunmuştur. Bu durumda sanal CPU talimatları disassembler araçları ile analiz edilerek sanal opcodlar haritalandırılmış ve çözümleme bu seviyede yapılmıştır.

Anti-debug mekanizmaları da sistemin önemli bir parçasıydı. SecuROM, IsDebuggerPresent(), NtQueryInformationProcess() gibi API çağrılarını kullanarak tersine mühendislik araçlarını tespit etmeye çalışır. Bu kontroller, kod içinden çıkarılarak veya sahte değerler döndürerek etkisiz hâle getirilmiştir. Structured Exception Handling (SEH) zincirleri, kontrol akışını karıştırmak için kullanılmış; ancak bu mekanizmalar da tersine mühendislik analizleriyle çözülmüştür. Sanal sürücü tespitine yönelik kontroller ise sistem kayıt defteri, dosya yolları ve process listesi üzerinden yapılmaktaydı. Korsan gruplar, bu izleri gizleyen Y.A.S.U. (Yet Another SecuROM Utility) gibi araçlarla sistemin sanal sürücüleri tanımasını engellemiş veya SecuROM'un kullandığı sürücüler üzerine sahte bilgiler yerleştirmiştir.

SecuROM'un 7.x ve üzeri sürümleri, lisans anahtarlarını donanım bileşenleri ile eşleştirerek online aktivasyon gerektiren bir yapı sunmuştur. Ancak bu sistemler de analiz edilerek, aktivasyon sürecinde sunucuya gönderilen HTTP paketleri incelenmiş ve yerel ağ üzerinde çalışan sahte aktivasyon sunucuları oluşturulmuştur. Alternatif olarak, EXE dosyası içerisindeki aktivasyon kontrol kodu doğrudan kaldırılmıştır. Bazı oyunlarda, korsan kullanım tespit edildiğinde oyun kendisini sabote edecek şekilde tasarlanmıştır (örneğin görevlerin ilerlememesi, kayıt dosyalarının bozulması gibi). Bu davranışlar da analiz edilerek oyunun içerik dosyaları (örneğin script ve veri tabloları) üzerinden kontrol noktaları bulunmuş ve işlevsiz hâle getirilmiştir.

Sonuç olarak, SecuROM'un sunduğu yüksek güvenlikli koruma katmanları, korsan gruplar tarafından çok aşamalı ve teknik açıdan karmaşık yöntemlerle bertaraf edilmiştir. Bu süreç, sadece yürütülebilir dosya patch'lemenin ötesine geçmiş; bellek analizi, sanallaştırma çözümlemesi, kernel düzeyinde manipülasyon ve sahte sunucu geliştirme gibi ileri düzey yazılım güvenliği zafiyetlerinin tespit ve istismarı yoluyla gerçekleştirilmiştir. Bu bağlamda, SecuROM'un kırılması, yazılım koruma sistemlerinin evriminde dönüm noktalarından biri olmuş ve daha sonra geliştirilen Denuvo gibi sistemlerin doğrudan bu deneyimlerden ders almasına yol açmıştır

"BioShock", "Mass Effect" ve "Spore" gibi oyunlar SecuROM koruması ile piyasaya sürüldü.1990'lı yıllarda oyun firmaları, korsanla mücadele etmek amacıyla çeşitli donanım ve

yazılım tabanlı koruma yöntemleri geliştirdiler. Ancak, bu yöntemler zamanla kullanıcı deneyimini olumsuz etkileyerek eleştirilere maruz kaldı. Bu durum, oyun firmalarının lisanslama stratejilerini yeniden gözden geçirmelerine ve daha kullanıcı dostu çözümler geliştirmelerine neden oldu.

4.3. 2000'ler – Dijital Dağıtımın Yükselişi ve Çevrimiçi Aktivasyonun Yaygınlaşması

2000'li yıllarda oyun lisanslama ve dijital dağıtım süreçleri, internetin yaygınlaşmasıyla birlikte köklü bir dönüşüm geçirdi. Bu dönemde, oyun firmaları korsanla mücadele etmek ve kullanıcı deneyimini iyileştirmek amacıyla çeşitli stratejiler benimsediler. Ancak, bazı uygulamalar kullanıcılar arasında ciddi tepkilere yol açtı.

4.3.1. Steam: Dijital Dağıtımda Devrim

Valve Corporation, 2003 yılında Steam platformunu piyasaya sürdü. Başlangıçta, Valve'ın kendi oyunları için otomatik güncellemeler sağlamak amacıyla geliştirilen bu platform, kısa sürede üçüncü taraf geliştiricilere de açılarak dijital oyun dağıtımında öncü hale geldi

Steamworks SDK, Valve'ın 2 Mayıs 2008'de tüm geliştiricilere açtığı kapsamlı bir yayın-ve-servis çerçevesiydi; bu tarihle birlikte Steam, yalnızca dijital mağaza değil, aynı zamanda entegre bir kimlik doğrulama ve kopya koruma altyapısı sunmaya başladı. Valve, Mart 2009'daki güncellemede "Custom Executable Generation" (CEG) adını verdiği katmanı ekleyerek her kullanıcı-makine ikilisine benzersiz, şifreli yürütülebilir dosyalar üretmeye başladı; böylece geleneksel seri numara denetimleri ya da sürücü tabanlı çözümlerden uzak, hesaba bağlanmış bir DRM mimarisi oluştu.

Teknik düzeyde Steamworks DRM üç temel bileşen üzerine kuruludur. İlk katman SteamStub'dur: oyun dosyalarini LZMA sıkıştırması eşliğinde AES-256 ile şifreler ve içine gömülü bir bütünlük imzası yerleştirir; program başlatıldığında Stub, Steam istemcisiyle yerel IPC üzerinden haberleşerek şifreyi çözmek için gereken anahtarı talep eder. İkinci katman SteamAPI/steamclient kitaplıklarıdır; burada ISteamUser::GetAuthSessionTicket() çağrısı kullanıcı oturumu için imzalı bir doğrulama bileti üretir, bileti geçersiz kılmak veya yenilemek de aynı arayüz üzerinden yapılır. Üçüncü katman olan CEG, Stub'ın çözdüğü kodu donanım parmak izine (CPU ID, sürücü seri numarası vb.) hash'leyerek makineye kilitler; farklı sistemde çalıştırılmaya çalışıldığında Stub bütünlük kontrolünü geçemediğinden uygulama kapanır.

Çalışma akışı şu şekilde işler: Steam istemcisi oyunu SteamPipe CDN'inden indirirken yürütülebilir hâl hâlâ Stub tarafından şifrelenmiştir; kullanıcı oyunu başlattığında Stub, geçerli hesabı doğrular, AES anahtarını belleğe alır, kodu sadece RAM'de çözer ve yürütmeyi başlatır. Çevrimdışı modda istemci, zaman damgalı bir lisans önbelleği tutar; bilet süresi dolana kadar internet gerekmez, ancak belirtilen süre (genellikle 30 gün) aşıldığında çevrim içi doğrulama zorunlu olur.

Bu çok katmanlı yaklaşım, klasik disk tabanlı korumalara göre kırılması güç bir engel seti oluşturdu. SteamStub'u tamamen soymak için geliştirilen Steamless gibi araçlar veya Steam API davranışını taklit eden Goldberg/SmartSteamEmu gibi emülatörler bulunmakla birlikte, Valve'ın her yama sırasında Stub imzasını yenilemesi ve CEG'nin kullanıcıya özel ikili üretmesi, korsan sürümlerin "gün 0"da piyasaya düşmesini önemli ölçüde geciktirdi.

Sonuç olarak Steamworks DRM, fiziksel medya odaklı SafeDisc-SecuROM döneminin ardından "hesap temelli" korumaya geçerek crack ekosisteminin saldırı yüzeyini kökten değiştirdi. Entegre başarımlar, bulut kayıtları, VAC ve Atölye gibi çevrim içi avantajlar korsan kopyaların cazibesini azaltırken, benzersiz yürütülebilir dosyalar ve sık güncellenen Stub şeması korsanlığın ekonomik etkisini, özellikle çıkış haftasında, kayda değer ölçüde sınırladı.

Ancak, Steam'in başlangıçta karşılaştığı bazı zorluklar da vardı. Örneğin, Half-Life 2'nin 2004'teki lansmanında, oyunun fiziksel kopyaları bile Steam üzerinden aktivasyon gerektiriyordu. Bu durum, sunucu yoğunluğu nedeniyle bazı kullanıcıların oyuna erişiminde gecikmelere yol açtı.

4.3.2. Ubisoft ve "Always-On" DRM Stratejisi

Ubisoft, 2010 yılında Uplay platformunu tanıtarak, oyunlarında sürekli internet bağlantısı gerektiren bir DRM sistemi uygulamaya başladı. Bu sistemde, oyuncuların tek oyunculu modda bile oyunu oynayabilmeleri için sürekli olarak Ubisoft sunucularına bağlı olmaları gerekiyordu.

Bu mimaride yürütülebilir dosya, Uplay Stub adlı bir kılıf içinde ile şifrelenerek; Stub açılışta Ubisoft Connect istemcisine TLS üzerinden donanım parmak izi (CPU ID, disk seri no. vb.) ve oturum açmış Ubisoft hesabını gönderiyor, sunucudan imzalı bir oturum jetonu alıyor ve gerçek kodu yalnızca RAM'de çözüyor. Oyunun bellekte düzenli aralıklarla (heartbeat) kimlik sunucusuna paket göndermesi, isteğin zaman damgası doğrulanamazsa yürütmenin durdurulmasına yol açıyordu.

Ayrıca sisteme istemci tarafında gömülü tarayıcı eklentisi de eklenmişti; ancak Temmuz 2012'de Google güvenlik mühendisi Tavis Ormandy'nin raporu, eklentinin komut satırı bağımsız değişkenini kötüye kullanarak rastgele dosya çalıştırılmasına izin verdiğini, yani pratikte bir "rootkit/back-door" açtığını gösterdi. Ubisoft aynı gün zorunlu yama yayımlamak zorunda kaldı.

Bu strateji, özellikle Assassin's Creed II ve Silent Hunter 5 gibi oyunlarda uygulandı. Ancak, 2010 yılında Ubisoft'un DRM sunucularına yapılan bir DDoS saldırısı sonucunda, bu oyunlar günlerce oynanamaz hale geldi

Kullanıcıların yoğun tepkileri üzerine, Ubisoft 2012 yılında bu politikasından vazgeçtiğini ve gelecekteki PC oyunlarında sürekli internet bağlantısı gerektirmeyeceğini açıkladı.

4.3.3. EA ve Spore: DRM Uygulamasının Ters Etkisi

Electronic Arts (EA), 2008 yılında piyasaya sürdüğü Spore oyununda, SecuROM adlı DRM yazılımını kullandı. Bu sistem, oyunun yalnızca üç farklı bilgisayara kurulmasına izin veriyor ve her kurulumda internet üzerinden aktivasyon gerektiriyordu. Ayrıca, SecuROM'un kullanıcıya bildirilmeden bilgisayara yüklendiği ve sistemde kalıcı değişiklikler yaptığı iddiaları ortaya atıldı

Bu uygulama, kullanıcılar arasında büyük bir tepkiye yol açtı. Amazon'da Spore, binlerce kullanıcı tarafından düşük puanlarla değerlendirildi. Ayrıca, EA'ya karşı toplu dava açıldı ve Spore, 2008 yılında en çok korsan olarak indirilen oyunlardan biri haline geldi.

EA, gelen tepkiler üzerine aktivasyon sınırını beş bilgisayara çıkardı ve de-aktivasyon aracı sunarak kullanıcıların lisanslarını başka bilgisayarlara taşımasına olanak tanıdı. Ancak, bu adımlar kullanıcı güvenini yeniden kazanmakta yetersiz kaldı.

Bu dönemde, oyun firmalarının korsanla mücadele amacıyla benimsedikleri bazı DRM stratejileri, kullanıcı deneyimini olumsuz etkileyerek ters tepti. Steam'in başarısı, kullanıcı dostu bir yaklaşımın önemini gösterirken, Ubisoft ve EA'nın yaşadığı olumsuzluklar, DRM politikalarının dikkatli bir şekilde planlanması gerektiğini ortaya koydu.

Bu gelişmeler, oyun endüstrisinde lisanslama ve kullanıcı deneyimi arasındaki dengenin ne kadar hassas olduğunu gözler önüne serdi.

5. GÜNÜMÜZDE KULLANILAN BAŞLICA OYUN LİSANSLAMA ÜRÜNLERİ

Oyun sektöründeki büyüme ve dijitalleşme, gelişmiş lisanslama yöntemlerinin ortaya çıkmasını ve kullanılmasını zorunlu hale getirdi. Korsan oyunların yaygınlaşması ile birlikte oyun geliştiricileri, gelişmiş DRM (Digital Rights Management) sistemlerine yatırım yapmaya başladılar. Günümüzde özellikle Denuvo, CodeMeter, Steamworks, Epic Online Services ve VMProtect gibi çözümler oyun sektöründe öne çıkan lisanslama teknolojileridir.

5.1. Denuvo Anti-Tamper Teknolojisi

Denuvo, 2014 yılında Avusturyalı Denuvo Software Solutions tarafından geliştirilen bir DRM teknolojisidir. Özellikle büyük bütçeli (AAA) oyunlarda tercih edilen bu sistem, oyunların korsan sürümlerinin çıkmasını aylarca geciktirme başarısı göstermiştir.

Denuvo, oyunların kodlarını sürekli olarak gerçek zamanlı şifreleme ve çözme süreçlerine tabi tutarak, yazılım korsanlarının bu kodları analiz ederek kırmasını zorlaştırır. Ayrıca

Denuvo, oyunların belirli bölümlerinin sürekli çevrimiçi olarak doğrulanmasını da sağlayabilir.

Temel bileşenlerden ilki SteamStub benzeri bir "stub" wrapperidir: oyun yürütülebiliri şifrelenip sıkıştırılır; stub yalnızca RAM'de çözülür ve özgün giriş noktasına aktarım yapılır. İkinci bileşen sunucu kaynaklı lisanslama sistemidir; program ilk açılışta CPU kimliği, disk seri numarası ve diğer donanım verilerini toplayarak Denuvo sunucusuna gönderir, karşılığında donanıma kilitli bir lisans dosyası alır ve yürütme sırasında eksik kod sabitlerini bu dosyada çözer. Üçüncü katman, seçilmiş kritik işlevleri Denuvo'ya özgü bir byte-koda çeviren sanal makinedir; talimat seti her yapımda değişir ve kayıt-bellek eşleşmeleri rastgele dağıtılır, bu da statik ve dinamik analizi büyük ölçüde zorlaştırır. Son katmanda sürekli bütünlük denetimi ve anti-debug önlemleri bulunur: kod bölümleri döngüsel olarak karma (CRC) testine tabi tutulur, kırpılmış veya değiştirilmiş handler tablosu saptanırsa uygulama kapanır ya da hatalı sabitler üretip çalışmayı bozar; ayrıca birkaç saniyede bir "heartbeat" paketleriyle lisans geçerliliği izlenir ve çevrimdışı mod yalnızca sınırlı süre sürer.

Uygulamanın çalışma zinciri şu adımlarla özetlenir: kurulum aşamasında şifreli stub diske yazılır; ilk çalıştırmada donanım kimliği ve oyun anahtarı sunucuya gönderilir, donanıma özgü lisans dosyası indirilir; oyun açıldığında sanal makine lisans verisini çözüp eksik sabitleri yerleştirir ve bütünlük döngüsü boyunca kendini denetler. Denuvo'nun ilk üç sürümü (2014-2016) tek katmanlı VM ve lisans dosyası yaklaşımına dayanıyordu; 2017'yle birlikte çift sarma (VMProtect içinde Denuvo) ve dinamik kod enjeksiyonuna geçildi; 2021 sonrasında Steam Deck/ARM desteği, su-işaretli TraceMark ve Nintendo Switch uyarlamaları eklendi. Her büyük sürüm, korsan grupların çözme süresini ilk başta haftalar veya aylar düzeyinde uzattı; ancak zamanla stub soyma araçları, lisans sunucusu emülatörleri ve VM de-virtualizer betikleri geliştirildi. Yine de her oyun yaması yeni stub imzası ve opcode haritası ürettiği için kırma araçları sürekli güncellenmek zorunda kaldı.

Kırılma teknikleri üç ana eksende ilerledi: şifreli kılıfın soyulup orijinal PE'nin yeniden inşası, sunucu uç noktasını taklit eden yerel lisans hizmetleri ve sanal makinenin talimat setinin haritalanarak gerçek x86 karşılıklarının otomatik üretilmesi. Örneğin Resident Evil Village'ın 2021'deki korsan sürümü, stub'u kaldırmakla kalmayıp bütünlük döngüsünü iptal ederek kare hızını da artırdı; benzer performans kazanımları, yoğun sanallaştırma ve CRC denetimlerinin CPU yüküne neden olduğunu gösterdi. Bununla birlikte Denuvo, çıkış haftasında korsan sürümlerin yayılmasını geciktirmeyi çoğu AAA yayınevi için kârlı kılmaya devam ediyor; ancak performans etkisi, çevrimdışı kısıtlar ve geçmişte yaşanan alan adı süresi dolma gibi operasyonel hatalar, geliştiricilerin her projede "koruma getirisi–kullanıcı memnuniyeti" dengesini yeniden tartmasını zorunlu kılıyor.

Kullanılan Oyun Örnekleri:

- FIFA Serisi (EA Sports)
- Doom Eternal (Bethesda Softworks)
- Resident Evil Serisi (Capcom)

Kullanıcılar arasında Denuvo’nun oyun performansını olumsuz etkilediğine dair yaygın tartışmalar mevcuttur. Denuvo kullanılan oyunların bazı durumlarda daha uzun yükleme sürelerine ve FPS düşüşlerine neden olduğu iddia edilir. Bu nedenle, oyun firmaları zaman zaman Denuvo'yu, oyunun ilk çıkış döneminde kullanıp, bir süre sonra kaldırarak oyuncuların tepkilerini azaltmayı tercih edebilmektedir.

5.2. CodeMeter Lisanslama Sistemi

CodeMeter, Almanya merkezli Wibu-Systems tarafından geliştirilen çok yönlü bir lisanslama ve DRM platformudur. Hem donanım (USB dongle) hem de yazılım tabanlı lisanslama seçenekleri sunan bu sistem, genellikle endüstriyel uygulamalarda, profesyonel yazılımlarda ve simülasyon oyunlarında tercih edilir.

CodeMeter, lisans verilerini özel bir donanım aygıtı veya güvenli bir yazılım kapsayıcısı içinde saklar. Yazılım, lisans kontrolü için bu güvenli kapsayıcıyı sorgular ve lisans doğrulanmadan yazılımı çalıştırmaz.

Kullanım Alanları:

- Endüstriyel simülasyon oyunları
- Profesyonel eğitim ve simülasyon yazılımları
- CAD/CAM mühendislik uygulamaları

CodeMeter, kullanımı kolay ve güvenilir bir çözüm olarak değerlendirilir. Ancak yüksek maliyeti nedeniyle daha çok profesyonel ve endüstriyel uygulamalarda tercih edilir.

5.3. Steamworks DRM Sistemi

Valve Corporation tarafından geliştirilen Steamworks, Steam platformunun entegre DRM çözümüdür. Oyuncuların Steam hesabına giriş yaparak lisans doğrulaması yapmasını sağlar.

Oyunlar, Steam platformu üzerinden satın alındıktan sonra kullanıcıların Steam hesaplarına bağlı kalır. Kullanıcılar, Steam hesabına giriş yaptıkları cihazlardan oyunlarını indirebilir ve çalıştırabilirler. Oyun başlatılırken internet üzerinden lisans doğrulaması yapılır.

Steamworks, kullanıcı dostu yapısı ve kullanım kolaylığı sayesinde oyuncular arasında oldukça popülerdir. Oyunların satın alımını, güncellemesini ve lisans yönetimini tek bir platformda toplayarak kullanım kolaylığı sağlar.

5.4. Epic Online Services (EOS)

Epic Games tarafından sunulan Epic Online Services (EOS), DRM ve lisanslama hizmetlerinin yanı sıra oyunların çevrimiçi hizmetlerini ve oyuncu yönetimini sağlayan bulut tabanlı bir platformdur.

EOS, oyunları bulut ortamında doğrular ve kullanıcının Epic hesabına giriş yapmasını zorunlu kılar. Kullanıcıların oyunlarının tüm platformlarda ortak bir şekilde yönetilmesini sağlar ve çevrimiçi hizmetleri kolaylaştırır.

Kullanılan Oyun Örnekleri:

- Fortnite (Epic Games)
- Rocket League (Psyonix)

Epic Games Store ve EOS, Steam'e alternatif bir platform olarak yükselmiş ve oyun dağıtımında rekabeti artırmıştır. Kullanıcı dostu özellikleri ve geliştiricilere sağladığı avantajlarla giderek daha fazla geliştirici tarafından tercih edilmektedir.

5.5. VMProtect Yazılım Koruma Sistemi

VMProtect, 2000'li yılların başında Rusya'da geliştirilen ve klasik "packer" yaklaşımlarının ötesine geçerek yürütülebilir dosyaları tersine mühendislik ile izinsiz değişikliğe karşı korumayı hedefleyen bir virtual machine-based anti-tamper çözümüdür. Araç, derleme sonrasında geliştiricinin seçtiği kritik fonksiyonları özgün x86-64 instructions dizisinden ayırır, her derlemede rastgele karıştırılan özel bir byte-code sözlüğüne dönüştürür ve bu kodu dosyaya gömülü küçük bir virtual CPU loop içinde AES-encrypted olarak saklar. Uygulama çalıştırıldığında stub bölümü yalnızca RAM üzerinde byte-code'u deşifre eder; ardından self-modifying, handler-tablosuz tasarlanmış yorumlayıcı, gerçek CPU yerine sanal talimatları adım adım yürütür. Bu süreçte periyodik CRC/HMAC integrity checks ve anti-debug APIs (ör. IsDebuggerPresent, NtQueryInformationProcess) devreye girerek bellek dökümü, breakpoint veya kod patch girişimlerini algılar, gerekirse uygulamayı kapatır veya "sabotaj" niteliğinde hatalı sabitler üreterek görev akışını bozar. VMProtect ayrıca yerleşik RSA-based licence system ile HWID-locked serial keys doğrular; böylece yazılımın hem statik patch'lenmesi hem de yetkisiz makinede çalıştırılması katmanlı şekilde engellenir. Sanal makine yorumlamasının getirdiği ek işlem yüküne rağmen, dinamik opcode karıştırması, güçlü şifreleme ve bütünlük döngüleri sayesinde tersine mühendislik masrafını önemli ölçüde artırır; saldırganın önce sanal talimat setini çözmesi, ardından şifreli byte-code'u yeniden geçerli machine code hâline dönüştürmesi gerekir. Bu nedenle VMProtect, hem bağımsız yazılım geliştiricileri hem de AAA oyun stüdyoları tarafından, performans-koruma dengesi gözetilerek tercih edilen ileri seviye bir software obfuscation and anti-tamper teknolojisi olarak öne çıkar.

Kısacası VMProtect, oyun kodlarını sanal bir işlemci üzerinde çalıştırarak gerçek işlemci üzerinde doğrudan çalışmasını engeller. Bu, korsan yazılımcıların oyun kodlarını analiz etmelerini ve değiştirmelerini ciddi şekilde zorlaştırır.

Kullanım Alanları:

- Özellikle Denuvo gibi DRM çözümleriyle birlikte kullanılır.

- Yüksek güvenlik gerektiren oyun ve uygulamalarda tercih edilir.

VMProtect, genellikle diğer DRM sistemlerini destekleyici olarak kullanılır ve performans üzerindeki etkisi, kullanıcılar tarafından minimum düzeyde olarak değerlendirilmektedir.

6. LİSANSLAMA ÜRÜNLERİNİN KARŞILAŞTIRILMASI VE ANALİZİ

Oyun sektöründe lisanslama teknolojisinin seçimi, yalnızca korsanla mücadele açısından değil; oyuncu memnuniyeti, geliştirme sürecinin verimliliği ve operasyonel maliyet açısından da kritik rol oynar. Bu nedenle firmalar, ihtiyaçlarına ve hedef kitlelerine uygun teknolojileri seçmek için mevcut çözümleri farklı boyutlarda değerlendirmelidir.

Aşağıda, en yaygın lisanslama çözümleri olan **Denuvo, CodeMeter, Steamworks, Epic Online Services (EOS)** ve **VMProtect** sistemleri karşılaştırmalı olarak analiz edilmiştir:

6.1. Güvenlik Seviyesi

Lisanslama Ürünü	Korsana Karşı Koruma	Kırılma Süresi	Ek Güvenlik Katmanı
Denuvo	Yüksek	Genelde 1-6 ay	Kod şifreleme, anti-debug
CodeMeter	Çok Yüksek	Nadir	Donanım Tabanlı Lisans Seçeneği
SteamWorks	Orta	Genelde 1-2 hafta	Steam istemcisine bağımlılık
EOS	Orta	Genelde 1-2 hafta	Hesap Doğrulaması
VMProtect	Destekeyici Katman		Kod obfuscation, sanal makine

CodeMeter ve Denuvo, korsana karşı en güçlü çözümleri sunar. CodeMeter donanım desteğiyle fiziksel düzeyde koruma sağlar. VMProtect, bağımsız olarak tam bir DRM değildir ama Denuvo gibi sistemleri güçlendirir.

6.2. Performans Üzerindeki Etkiler

Lisanslama Ürünü	FPS Düşüşü	Yükleme Süresi	Arka Plan İşlemleri
Denuvo	Bazi Oyunlarda Hissedilir	Artabilir	Sürekli Runtime Kontrol
CodeMeter	Minimum	Değersiz	Düşük sistem yükü

Steamworks	Düşük	Stabil	Steam Üzerinden Doğrulama
EOS	Düşük	Stabil	Epic Sunucusuna Bağlanma
VMProtect	Değişken	Kod Büyüklüğüne Bağlı	Sanal makine çalışması nedeniyle hafif gecikme olabilir

Performans açısından CodeMeter ve Steamworks daha kullanıcı dostudur. Denuvo'nun bazı oyunlarda FPS düşüşlerine sebep olduğu bağımsız testlerle belgelenmiştir. VMProtect ise geliştirici kullanımına ve kod mimarisine bağlı olarak değişken sonuçlar doğurabilir.

6.3. Kullanım Kolaylığı ve Entegrasyon

Lisanslama Ürünü	Geliştirici için Kurulum	Oyuncu Deneyimi	Platform Desteği
Denuvo	Karmaşık SDK Lisans Gerekir	Tartışmalı	PC (Bazı Konsollar)
CodeMeter	Detaylı Yapılandırma Gerekir	Stabil	Çoklu Platform
Steamworks	Kolay, entegre sistem	Oyuncu Dostu	PC (Steam)
EOS	Orta Düzey Entegrasyon	Basit Arayüz	PC + Konsollar
VMProtect	Teknik Bilgi Gerekir	Kullanıcı Farketmez	Windows Ağırlıklı

Steamworks ve EOS, geliştirici entegrasyonu açısından en kolay ve hızlı çözümlerdir. Özellikle bağımsız geliştiriciler için idealdir. Denuvo ve CodeMeter daha fazla teknik bilgi ve yatırım gerektirir. Oyuncu deneyimi açısından Steam halen liderdir.

6.4. Maliyet Analizi

Lisanslama Ürünü	Lisans Ücreti	Geliştirme Süresine Etki	Ticari Ölçek
Denuvo	Yüksek	Artar	AAA Oyunlar
CodeMeter	Orta-Yüksek	Artar	Profesyonel Yazılımlar

Steamworks	Ücretsiz	Azaltır	Yaygın
EOS	Ücretsiz	Az düzeyde arttır	Orta-Büyük Stüdyolar
VMProtect	Düşük-Orta	Teknik destek gerekebilir	Küçük-Orta Ölçek

*Steamworks kullanımı ücretsizdir, ancak Steam satış gelirlerinden %30'a kadar komisyon alır.

Maliyet açısından bakıldığında Steamworks ve EOS, oyunlarını geniş kitlelere ulaştırmak isteyen geliştiriciler için düşük giriş bariyeri sağlar. Denuvo ve CodeMeter ise yüksek güvenlik gereksinimi olan, AAA düzeyde ürünler için tercih edilir.

7. YENİ NESİL LİSANSLAMA YAKLAŞIMLARI VE GELECEK TRENDLERİ

Teknolojinin evrimiyle birlikte geleneksel yazılım lisanslama yöntemleri, özellikle oyun sektöründe yeterli koruma, esneklik ve kullanıcı dostu deneyim sağlayamaz hale gelmiştir. Bu nedenle oyun firmaları, hem korsanla mücadele edecek hem de kullanıcı deneyimini bozmadan sürdürülebilir gelir modelleri sunacak yeni yaklaşımlar üzerinde yoğunlaşmaktadır.

7.1. Blockchain Tabanlı Lisanslama ve NFT'ler

Blockchain teknolojisi, merkeziyetsiz ve şeffaf yapısı sayesinde lisans bilgilerinin güvenli ve değiştirilemez bir şekilde saklanmasını sağlar. Oyun sektöründe bu teknoloji, lisansların ve oyun içi öğelerin doğrulanabilir dijital varlıklar (NFT'ler) olarak tanımlanmasını mümkün kılar.

Enjin, Gala Games, Ultra gibi blockchain tabanlı oyun platformları, oyun içi varlıkları NFT formatında sunarak oyunculara gerçek mülkiyet sağlıyor.Oyun lisansları da NFT olarak kullanıcıya atanabilir, böylece ikinci el oyun satışı gibi kavramlar dijital ortamda şeffaflıkla yürütülebilir.

Olası Kazanımlar:

- Kullanıcının oyunlar ve içerikler üzerindeki mülkiyet duygusunu artırır.
- Lisanslar transfer edilebilir hale gelir.
- Korsan kullanım yerine kayıtlı cüzdan sahipliği doğrulanır.

Zorluklar:

- Enerji tüketimi (Proof-of-Work sistemlerde)

- Oyuncular ve geliştiriciler arasında “gerçek sahiplik” kavramının hukuki netliğe kavuşmaması

7.2. Abonelik ve Hizmet Olarak Oyun (Game-as-a-Service)

Oyunlar artık tek seferlik satın alınan ürünler yerine, abonelik modeliyle sunulan sürekli güncellenen servisler haline geliyor. Lisanslama bu durumda abonelik süresiyle sınırlı hale geliyor.

Örnekler:

- Xbox Game Pass
- PlayStation Plus Extra/Premium
- Ubisoft+
- NVIDIA GeForce NOW (streaming tabanlı)

Avantajlarından bahsedecek olursak Geniş kütüphanelere düşük maliyetle erişim öne çıkan en önemli avantaj diyebiliriz. Ayrıca lisasın süreli olması korsan kullanımını anlamsız hale getiriyor ve oyunculara oyunları deneme özgürlüğü sunuluyor. Geliştirici açısından ise sürekli gelir akışı sağlıyor ve oyunun topluluk etkileşiminin artmasına katkı sağlıyor buda oyunun ömrünü uzatıyor.

7.3. Yapay Zeka Destekli Lisans İzleme ve Koruma

Gelişmiş yapay zekâ algoritmaları, yazılımın olağan dışı kullanım kalıplarını gerçek zamanlı olarak analiz ederek korsan kullanım şüphesi taşıyan davranışları tespit edebilir. Bu sistemler geleneksel DRM’lerin yerine değil, onları tamamlayıcı olarak kullanılır.

Örnek Potansiyel Uygulamalar:

- Lisansın olağandışı coğrafi hareketliliğini tespit etme (VPN + paylaşım senaryoları)
- Aynı anda çok cihazdan erişimi algılama
- Anormal oturum süresi ve davranış örüntüsü tespiti

Bu sistemlerin kullanımı, kullanıcı davranışına göre adaptif lisanslama modelleri (örneğin sadık kullanıcılara esneklik tanıyan, korsana eğilimli kullanıcılarda daha sıkı kontrol uygulayan sistemler) oluşturulmasını mümkün kılabilir.

7.4. Platform Bağımsız Lisanslama ve Bulut Oyun Geleceği

Lisanslamada bir diğer eğilim, oyunun çalıştığı cihaza değil kullanıcıya atanmasıdır. Bulut oyun hizmetleri, fiziksel donanımı ortadan kaldırarak lisansın tamamen kimlik temelli doğrulanmasını mümkün kılar.

- Google Stadia (artık kapatıldı) ve Xbox Cloud Gaming, lisansın donanıma değil hesaba bağlı olduğu örneklerdir.
- Gelecekte oyun lisansı = bulut kimliği = kullanıcı cüzdanı olabilir.

Avantaj:

- Donanım korsanlığı tamamen önlenir
- Lisans yönetimi çok daha merkezi ve güvenli hale gelir.

7.5. Kullanıcı Odaklı Lisanslama Politikaları

Kullanıcıların DRM karşıtı tepkileri, firmaların daha şeffaf, performans dostu ve kullanıcı haklarına duyarlı lisanslama sistemlerine yönelmesine neden olmuştur. Bu alandaki gelişmeler:

- DRM'siz platformların (örneğin GOG.com) yükselişi
- Açık lisans ve offline oynama seçeneklerinin desteklenmesi
- Kullanıcılar tarafından kötü niyetli olarak algılanabilecek "always online DRM" gibi uygulamalardan kaçınılması.

Yeni nesil lisanslama çözümleri, geçmişin katı DRM sistemlerinden daha esnek, kullanıcı dostu ve teknolojiye entegre yaklaşımlar sunmaktadır. Bu geçiş sürecinde geliştiricilerin en büyük başarısı, korsan yazılımla mücadele ederken kullanıcı deneyiminden ödün vermemeyi başarmak olacaktır.

8. OYUN GELİŞTİRİCİLERİ İÇİN LİSANSLAMA STRATEJİLERİ VE TAVSİYELER

Lisanslama teknolojisinin başarısı yalnızca korsan yazılımı önlemekle değil, aynı zamanda oyunun kullanıcı deneyimini, teknik sürdürülebilirliğini ve ekonomik verimliliğini de koruyabilmesiyle ölçülür. Bu nedenle bir oyun geliştiricisinin, lisanslama stratejisini belirlerken ürün tipine, hedef kitleye ve dağıtım kanallarına göre çok yönlü bir değerlendirme yapması gerekir.

8.1. Oyun Türüne ve Bütçeye Göre Lisanslama Stratejisi

AAA (Yüksek Bütçeli) Oyunlar

- Tavsiye Edilen Sistem: Denuvo + VMProtect gibi yüksek güvenlikli, kırılması zor sistemler.
- Neden: İlk satış dönemleri kritik olduğundan korsan kopyaların geciktirilmesi ekonomik açıdan büyük önem taşır.
- Dikkat: Performans üzerindeki etkiler için optimizasyon yapılmalı ve belirli bir süreden sonra Denuvo kaldırılması değerlendirilebilir.

Orta Ölçekli ve Indie Oyunlar

- Tavsiye Edilen Sistem: Steamworks, EOS gibi entegre ve düşük maliyetli çözümler.

- Neden: Korsanla savaşta sınırlı kaynaklar varken, erişilebilirlik ve kullanıcı deneyimi öncelikli olmalı.
- Dikkat: Aşırı DRM kullanımı, küçük çaplı oyunlarda kullanıcı tepkisini artırabilir.

Eğitim ve Simülasyon Oyunları

- Tavsiye Edilen Sistem: CodeMeter veya benzeri donanım/yazılım hibrit sistemleri.
- Neden: Profesyonel kullanımda lisans takibi, yetkilendirme ve offline kullanım senaryoları kritik olabilir.

8.2. Yayın Öncesi ve Sonrası DRM Stratejisi

Yayın Öncesi: DRM sistemleri entegre edilirken kullanıcı testleriyle birlikte performans ve kullanıcı erişim senaryoları analiz edilmelidir.

Yayın Dönemi: Korsanla savaş için Denuvo gibi çözümler etkili olabilir; ancak sosyal medya ve oyun basınında olumsuz PR riskine karşı hazırlıklı olunmalıdır.

Yayın Sonrası: İlk birkaç ay içinde korsan koruma kaldırılarak performans artırımı yapılabilir ve kullanıcı geri bildirimi iyileştirme için kullanılabilir.

8.3. Lisanslama Sürecinde Kaçınılması Gereken Hatalar

1. Always-Online DRM'yi Zorunlu Kılmak:
   Oyuncular çevrimdışı oynama özgürlüğüne önem verir. Sürekli bağlantı gerektiren sistemler, hizmet kesintilerinde büyük tepki alabilir (örneğin Ubisoft 2010 örneği).

2. Gizli Yazılım Yüklemek veya Şeffaf Olmamak:
   SecuROM gibi sistemler, sistem düzeyinde müdahaleler yaptığı için ciddi güvenlik ve gizlilik sorunları yaratmıştır. Kullanıcıya tam bilgilendirme şarttır.

3. DRM'yi Performansla Takas Etmek:
   Oyun motoruna entegre edilen DRM katmanları, optimizasyon yapılmadan bırakılırsa FPS düşüşleri ve yüksek RAM kullanımı gibi sorunlar yaratabilir.

8.4. Lisanslama Süreci İçin İyi Uygulamalar

- Minimum Gereklilik İlkesi: Oyunun çalışması için yalnızca en gerekli lisans kontrolü yapılsın. Fazla kontrol, kullanıcıyı üründen soğutur.
- Modüler DRM Entegrasyonu: DRM sistemleri, oyunun diğer modüllerinden bağımsız ve kolay güncellenebilir şekilde tasarlanmalıdır.
- Lisanslama Metodolojisinin Belgelendirilmesi: Lisans kontrol algoritmaları, teknik dokümantasyonla desteklenmeli ve sürüm kontrolüne tabi tutulmalıdır.
- Toplulukla Şeffaf İletişim: Oyuncular neden bir DRM kullanıldığını anladığında daha anlayışlı olabilir. Açık iletişim, güven oluşturur

8.5. Alternatif Yaklaşımlar

Bazı bağımsız geliştiriciler ve açık kaynak oyun toplulukları, korsanla savaşmak yerine oyuncuya güvenerek erişim kolaylığı sunmayı tercih etmektedir. Bu yaklaşım özellikle hikâye odaklı ya da küçük bütçeli projelerde, oyuncuların olumlu geri dönüşleri ve bağışlarıyla sürdürülebilir hale gelebilmektedir. Örneğin GOG.com üzerinden DRM'siz sunulan oyunlar, kullanıcı sadakatine dayalı bir satış modeli oluşturarak uzun vadeli başarı sağlamıştır.

Lisanslama stratejisi, oyunun türü, hedef pazarı ve teknik yapısı dikkate alınarak özel olarak tasarlanmalıdır.
Korsan yazılımı önleme çabası, oyuncunun memnuniyetine zarar verecek bir noktaya taşınmamalıdır.
Geliştirici ve oyuncu arasında güvene dayalı şeffaf bir ilişki kurmak, korsana karşı en güçlü stratejilerden biridir.

9. SONUÇ VE GENEL DEĞERLENDİRME

Yazılım dünyasında lisanslama, özellikle oyun sektöründe yalnızca hukuki bir zorunluluk değil, aynı zamanda bir ekonomik güvenlik kalkanıdır. Bu araştırmada, oyun sektörünün lisanslama süreçlerinde yaşadığı evrimsel süreci kronolojik olarak incelenmiş ve geçmişten günümüze kullanılan yöntemleri, teknolojileri, bunların oyuncu deneyimi üzerindeki etkilerini ve geliştiricilerin karşılaştığı zorlukları ortaya koyulmuştur.

9.1. Ana Bulgular

- **1980'li yıllar**, basit seri numaraları ve fiziksel koruma materyalleriyle korsana karşı ilk savunmaların başladığı dönemdi. Bu çözümler basitti ama kısa sürede etkisiz hale geldi.
- **1990'lı yıllar**, donanım tabanlı korumalar (dongle) ve disk odaklı DRM sistemlerinin denendiği dönemdi. Güvenliği artırsa da kullanıcı dostu değildi.
- **2000'li yıllar**, Steam gibi platformların çevrimiçi lisanslama ve otomatik güncellemeleri bir araya getirdiği dijital devrim dönemiydi. Ancak aynı zamanda agresif DRM uygulamaları (örneğin Spore'da SecuROM) kullanıcı tepkilerini artırdı
- **2010 sonrası**, Denuvo gibi sofistike DRM teknolojilerinin yükselişi, korsanı geciktirmeyi başarsa da performans sorunları nedeniyle tartışmalı hale geldi.
- **2020 ve sonrası**, daha kullanıcı odaklı, şeffaf ve dijital mülkiyete dayalı yeni lisanslama anlayışlarının şekillenmeye başladığı bir dönemdir. Blockchain, NFT, yapay zekâ ve bulut lisanslama gibi teknolojiler öne çıkmaktadır.

9.2. Stratejik Öneriler

- **Kapsayıcı Yaklaşım:** Geliştiriciler korsanla savaşırken kullanıcı deneyimini ihmal etmemelidir. Aksi halde yasal yoldan satın alma isteği yerine ters etki yaratılabilir.
- **Esneklik ve Sadelik:** DRM sistemlerinin sade, hızlı, düşük sistem yükü oluşturan yapılarla uygulanması kullanıcı memnuniyetini artırır
- **Şeffaflık ve İletişim:** DRM kullanımı açıkça ve dürüstçe oyuncuya anlatıldığında, oyuncuların toleransı artmakta, firma-oyuncu güven ilişkisi kuvvetlenmektedir.
- **Geleceğe Hazırlık:** NFT, bulut lisanslama ve platformlar arası dijital kimlik doğrulama sistemleri, lisanslamanın geleceğini oluşturacak kritik bileşenlerdir.

9.3. Sonuç

Lisanslama sistemleri artık sadece bir koruma kalkanı değil; aynı zamanda oyunun ticari başarısını ve oyuncu bağlılığını doğrudan etkileyen bir deneyim tasarımı unsurudur. Başarılı bir lisanslama yaklaşımı, sadece korsanı önlemekle kalmaz, aynı zamanda oyunun kullanıcı gözünde daha erişilebilir, güvenilir ve kalıcı bir dijital ürün olarak algılanmasını sağlar.

Oyun sektörü geliştikçe, lisanslama sistemlerinin de daha etik, kullanıcı odaklı ve teknolojiye entegre çözümler sunması kaçınılmazdır. Geleceğin oyunları, sadece nasıl oynandıklarıyla değil, nasıl korunduklarıyla da hatırlanacaktır.

Referanslar

- [ ] https://www.youtube.com/watch?v=HjEbpMgiL7U
- [ ] https://en.wikipedia.org/wiki/SafeDisc
- [ ] https://en.wikipedia.org/wiki/SecuROM
- [ ] https://github.com/MrKristofere/SmartSteamEmu
- [ ] https://www.ubisoft.com/en-us/ubisoft-connect
- [ ] https://www.technopat.net/2016/03/22/denuvo-kopya-korumasi-nedir/
- [ ] https://www.wibu.com/products/codemeter/runtime.html
- [ ] https://www.mobygames.com/group/16350/games-with-hardware-dongle-copy-protection/
- [ ] https://www.youtube.com/watch?v=VQ6uz6nJcfI
- [ ] https://www.youtube.com/watch?v=Mv7wm4no2Cw
- [ ] https://retrocomputing.stackexchange.com/questions/6170/origin-of-copy-protection-dongles
- [ ] https://www.youtube.com/watch?v=3qBacrWnbtA
- [ ] https://www.lucadamico.dev/papers/drms/safedisc/MidtownMadness.pdf
- [ ] https://www.pcgamingwiki.com/wiki/SecuROM
- [ ] https://en.wikipedia.org/wiki/Steam_(service)
- [ ] https://www.pcgamingwiki.com/wiki/User%3ACyanic/Steam_DRM
- [ ] https://partner.steamgames.com/doc/api/isteamuser
- [ ] https://en.wikipedia.org/wiki/Always-on_DRM
- [ ] https://www.forbes.com/sites/adriankingsleyhughes/2012/07/30/hacker-claims-ubisoft-uplay-drm-is-a-rootkit-and-poses-security-risk/
- [ ] https://connorjaydunn.github.io/blog/posts/denuvo-analysis/
- [ ] https://en.wikipedia.org/wiki/Denuvo
- [ ] https://dev.epicgames.com/docs/epic-online-services/eos-overview
- [ ] https://vmpsoft.com/vmprotect/overview
- [ ] https://cfp.recon.cx/recon2024/talk/YQK3FK/
- [ ] https://github.com/JonathanSalwan/VMProtect-devirtualization
- [ ] https://blog.back.engineering/17/05/2021/