Best Practices For Game Developers: Protecting your Product

June 2004

macrovision®

Table of Contents

Introduction

It is getting more expensive to produce games. Margins for error are being squeezed tighter, directly impacting profit margins and production schedules.

The production budgets of yesterday are no longer sufficient to fund development of today's games.

Where will funding money come from? The Electronic Software Association (ESA) recently estimated that, in the U.S. alone, games revenues lost to Piracy would have funded the development of over one thousand, six hundred new high quality games.

Combating the losses caused by 'casual copying' and 'software cracking' requires a combined approach: (1) adequate legislation, (2) technology that can defend a game without compromising development or game play, and (3) a better understanding of the methods used by software pirates and hackers.

Highlights

Combating the losses caused by 'casual copying' and 'software cracking' requires a combined approach: (1) adequate legislation, (2) technology that can defend a game without compromising development or gameplay, and (3) a better understanding of the methods used by software pirates and hackers.

New Piracy Challenge

According to the ESA, worldwide packaged media piracy is estimated to have an annual cost to the U.S. entertainment software industry of over $3.0 billion in each of the past several years. This estimate includes the piracy impact from rogue replication plants in countries on the International Intellectual Property Alliance (IIPA) priority watch list, but does not account for revenues lost from pirated copies downloaded from online sources. Accounting for piracy losses from online sources, one could safely assume the number to be much greater. These losses will undoubtedly continue to increase if measures are not taken to minimize the negative impact of online piracy.

Today, even the most marginal of software game titles are freely available from various Internet sources. In fact, most titles are posted even before the official release date. This is called the "0 day crack" and it is a badge of honor for any cracking group. The worldwide reach of the Internet, combined with the rapid growth of high-speed connections to homes and universities, has provided a mass-market distribution channel reaching millions of software users. Improvements in user-friendly tools that simplify finding and downloading files have pushed the process into the mass market. Although the media focus on peer-to-peer (P2P) piracy has revolved around the music industry, music was simply the first media form to experience the impact of online piracy. This is largely a matter of the smaller music file size compared with other media types. The music piracy demographic is also a major consumer of videos and video games. Provide this demographic with better, faster broadband access, and it no surprise that illegal video and video game distribution would be next on their agenda.

Software Games may appear online as 'disc images' for download and installation, or as 'cracked' executables that requires some minor installation and positioning by the user. Years of development team effort can be lost in seconds if game code is not protected, or is released into the public domain without adequate safeguards.

Millions of pounds on development, manufacturing, distribution, promotion and technical support can be lost if a single evaluation copy is mislaid.

Highlights

The sales cycle of entertainment software is consistent with other entertainment media – the majority of sales occur in the first 6 to 8 weeks of release and the shelf life is typically less than one year.

The sales cycle of entertainment software is consistent with other entertainment media – the majority of sales occur in the first 6 to 8 weeks of release, and the shelf life is typically less than one year. When a Triple "A" title that sells for £30 to £40 can be found online soon after release, many users are naturally tempted to download the free (cracked) game, cannibalizing sales.

Do not compromise security

Interactive software games possess an inherent security advantage over other forms of entertainment media: it is software. With software, security capabilities can be integrated into the code, adding multiple layers of security, and increasing the time and effort a hacker must apply to circumvent the security. The goal of these efforts is to augment and extend the viable retail window of the title.

Security should never be compromised in a rush to meet other production milestones. All development timetables need to anticipate implementing appropriate security measures, both within the 'real world,' and within the software application itself.

The Developer & Publisher should therefore perform a rudimentary risk-assessment to determine what level of protection is required for their game, whilst it is still in development. The responsibility for addressing the threats revealed in such a risk-assessment will then need to be allocated.

Triple-A games that are projected to sell in the hundreds of thousands clearly face a significantly higher risk than their more stealthy niche game counterparts.

For certain titles, Publishers may feel that incorporating post-production 'copy protection wrappers' will offer sufficient protection against lost revenues. In cases where the risk to revenues is determined to be higher, copy protection wrappers may require complementary ‘anti-hack’ technologies, integrated into the code by the Developer during production.

As recently as May 2004, Macrovision witnessed a leading games publisher gain twenty days of hack-free retail sales for a 'triple A' title after an investment of only two days of security API integration.

Highlights

As recently as May 2004, Macrovision witnessed a leading games publisher gain twenty-one days of hack-free retail sales for a 'triple A' title after an investment of only two days of security SDK integration.

Protect your game’s lifecycle

As explained above, Game Publishers and Developers need to work together to ensure that their games are sufficiently protected during their retail life cycle. This involves adopting a “cradle to grave” perspective.

Developers need to know that their core code is secure as they develop their products. Testing programs need to be undertaken in a controlled manner to ensure that alpha or beta code is not released into the public domain. Early releases that have not been copy-protected can form the basis of future cracks when the final product ships.

When a finished game is shipped to Publishers, and ultimately to CD-replication facilities, care must be taken to observe that internal security is not compromised. It is not unknown for some hack sites to publish financial rewards for the successfully delivery of a finished game product.

The retailer must also observe strict security protocols when they receive advance shipments of stock. For example, games should not be available to staff to purchase or remove from the premises prior to the official launch date and time.

In addition to these areas, care must be taken by the Developer and Publisher when they issue software updates for released products. Software updates require the same level of protection as retail products.

Solution – Schedule security into development plan

Game publishers and developers are starting to recognise the need to schedule security into their project plans. Building upon the ‘risk-assessment’ discussed earlier, the following should be kept in mind when considering the need for hack protection security:

Return – Consider the popularity of the game titles. What is the current forecast and past sales performance? How much in incremental sales would be achieved with an extra week, two weeks, or four weeks? Is the return greater than three (3) days of development effort?

Project Scheduling – When is the best time to start the security integration? The ideal timeframe is between 6 months prior to release to as little as 6 or 8 weeks. Who would be the security lead in your developer organization?

Testing / QA – How can QA be prepared to test the modified behavior, or to recognize the security in the source code without generating false positives?

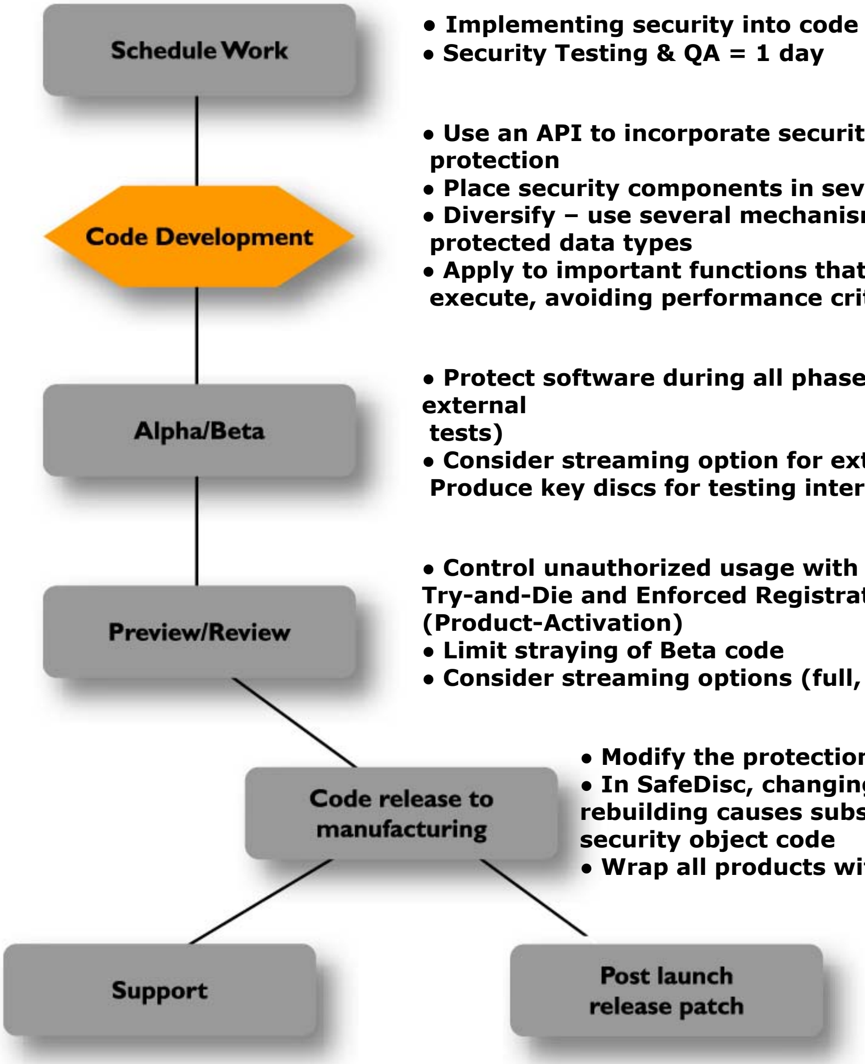
Controlling Pre-Release Reviews and Promotions – There a number of ways by which pre-release review programs can be undertaken in a controlled manner. Applying a unique serial number per review publisher may help track pirated copies back to their source. Unfortunately, this may be too little, too late to prevent mass distribution. A more powerful solution is to adopt a 'product-activation' technology that ties the application to be reviewed to a specific computer. Product-activation code that creates an 'electronic-license' can be sourced from Macrovision and other companies. Once 'activated' an application suffers no performance or game play penalty. If copied to a CD or to another system, the title will simply not function. This technology can be applied to 'rented' games, and allows publishers to obtain accurate business intelligence about product usage (e.g. how many customers have activated their products, and at what rates).

Support – It is important to educate technical support staff regarding the identifiable behaviour of cracked versions, permitting the staff to distinguish between a real version and a cracked one. This will help focus support's resources on genuine inquiries from legitimate consumers.

Highlights

It is important to educate technical support staff regarding the identifiable behaviour of cracked versions, permitting the staff to distinguish between a real version and a cracked one. This will help focus support's resources on genuine inquiries from legitimate consumers.

Best Practices



- Implementing security into code = 2 days
- Security Testing & QA = 1 day

- Use an API to incorporate security into software code for protection
- Place security components in several functions
- Diversify – use several mechanisms like SafeDisc's protected data types
- Apply to important functions that contain code that must execute, avoiding performance critical routines

- Protect software during all phases of test (internal & external tests)
- Consider streaming option for external testers
  Produce key discs for testing internally

- Control unauthorized usage with some form of activation, Try-and-Die and Enforced Registration for reviewers (Product-Activation)
- Limit straying of Beta code
- Consider streaming options (full, hybrid)

- Modify the protection from beta
- In SafeDisc, changing encryption seeds, then rebuilding causes substantial changes to the security object code
- Wrap all products with a unique license

- Provide known issues of copy protection components technology to your Support Team In advance of product release

- Notify of any intentional behavior modifications that can assist support in identifying cracked version over the phone

- Activate any unused security
- Add new security component

Business Challenge

Highlights

Fifteen percent of the people surveyed had acquired in excess of fifteen pirated games in that period.

The games industry is well aware that the Internet is used to distribute hacked versions of games. These hacks come in many forms, from cracked disc images that get burned straight to CD-ROM, to the core .exe file that replaces the file stored on a user's hard disk. A recent survey of PC games players illustrated that forty six percent of respondents had acquired pirated games in the last two years[1]. Fifteen percent of the people surveyed had acquired in excess of fifteen pirated games in that period.

Research also indicates that the number of skilled hackers is miniscule compared with the number of users who download and re-distribute these files. Denying unauthorized access to unprotected games is the first step towards reducing the availability of cracked versions online. The initial responsibility, therefore, lies with the developer.

Surprisingly, some developers see the issue of 'copy-protection' as the sole responsibility of the publisher who buys the rights and intellectual property of a completed game. Whilst a publisher can certainly opt to apply a security layer post-production, this is effective only against casual consumer copying. Developers themselves are the group best suited to defending a game from being hacked through tighter integration between the game and security measures.

Building effective copy-protection starts with the Developer. It involves: 1. designing defences into the game that impede or mislead hackers; 2. ensuring that access to development, such as alpha & beta testing, is strictly controlled; 3. closer cooperation with publishers and manufacturers.

Protecting a game is like many things in life - the more effort you put in, the better the result. In the pressured world of game development, it is a more than a travesty when the efforts and costs of developing a triple-A game are overshadowed by the pre-release appearance of an online cracked version. In this ecosystem, all members need to take responsibility and protect each other.

[1] Macrovision Survey of 2219 online respondents – May 2004

Contact Information

Macrovision Corporation
2830 De La Cruz Blvd.
Santa Clara, CA 95050
United States
Phone: +1 (408) 743 8600
Fax: +1 (408) 743 8610

Macrovision UK Ltd.
14/18 Bell Street
Malvern House
Maidenhead
SL6 1BR
United Kingdom
Phone: +44 (0)870 871 1111
Fax: +44 (0)870 871 1161

Macrovision Japan and Asia K.K.
Takaba Bldg. 2F
2-18-5, Jingumae, Shibuya-ku
Tokyo 150-0001
Japan
Phone: +81 (0)3 5774 6253
Fax: +81 (0)3 5774 6269

www.macrovision.com