Winning The Race Against Software Pirates

Next Generation Copy Protection

Yours Truly

Erik Simon

- Veteran of the German Development Community, started out in 1988.
- Has worked in nearly all development jobs, except hardcore programming.
- Companies: Thalion, Blue Byte, JoWooD, currently Sunflowers.
- Head of Development Position for the last 5 years.

Topics

- Why the entertainment software industry is more threatened by piracy than ever, and why it has better chances to do something about it as other entertainment industries.
- The Pirate Scene - Know Your Enemy
  A Crackers motivation. The structure of the current piracy scene.
- Principles of better copy protection and methods of implementation.
- Sharing practical experiences:
  Ensuring compatibility and as small a time commitment of the development team as possible. Testing and evaluating copy protection technology.
- Establishing a better protection in your organization: Non-technical problems and solutions.
- The Vision:
  Noticeably better sales by a broad use of better copy protection technology, or: why all of us will profit when more major players use better copy protection.

Effective Copy Protection – A Dream ?

- At first, this topic seems to be a tired one…
- Since over 20 years, the struggle against software piracy appears to be a failure.
- Most of the time, there are pirated copies of our games available simultaneously to street release.
- „*But we tried everything!*“ – Have we really?
- „*Isn‘t worth the effort.*“ Hesitations:
  - Being cracked in days renders copy protection useless.
  - Dev team mostly hasn’t got the necessary skills.
  - Afraid of falling behind schedule because of problems with copy protection and it’s testing.
- Standard copy protection is usually applied, thus combining compatibility problems with a useless protection level.

Between A Rock And A Hard Place

Why the issue of copy protection is more valid than ever

A short history in order to see the bigger picture:

- Home Computer format live cycles were shortened not only by new technology, but also due to pressure by piracy on established platforms.
- Especially interesting: The downfall of the Amiga. Game sales plunged and the industry moved on to a platform that was then still technologically inferior: the PC.
- Soon, there were crack patches and disk copy programs on the PC. The CD-ROM came to the rescue (and was also a driving force technologically, of course).
- The CD gave us some brief golden years. As long as CD-writers and blank CDs were not on a consumer price level, sales also for non-hyped titles reached break even much more often.

Between A Rock And A Hard Place

Why the issue of copy protection is more valid than ever

- So: Whenever the piracy pressure grew unbearable on a format, we moved on to another platform or another data carrier.
- Problem: We can't do this anymore.
  - The PC as a home computer gaming platform is here to stay. (thank goodness for that!)
  - Exclusive use of the DVD is not a solution, since:
  - Still, not everybody has a DVD-drive.
  - DVD-writers and blanks arrived at consumer price level.
  - The Piracy Scene releases "rips" – these are shrunken versions of a game done by removing unnecessary data or compressing them.
- Copying is not nerd wizardry anymore.
  - Through many articles in the print press or on websites, copying a CD or downloading a complete game with a file sharing client is now common knowledge.

Between A Rock And A Hard Place

Why the issue of copy protection is more valid than ever

Damage

- What's the actual damage done by piracy to our industry? Hard to say.
- Reliable numbers for the game industry are not available to my knowledge. The BSA released figures for 2001 for all software areas: $2,7 Billion in Western Europe alone and $1,9 Billion in the US.
- Take a look at your surrounding: copying or downloading games and other media is routine…
- Use some common sense: if your sales would only gain 10% (and that's a low estimate), this gives you some serious budget to buy and to create copy protection technology.

The „Scene“
Know Your Enemy

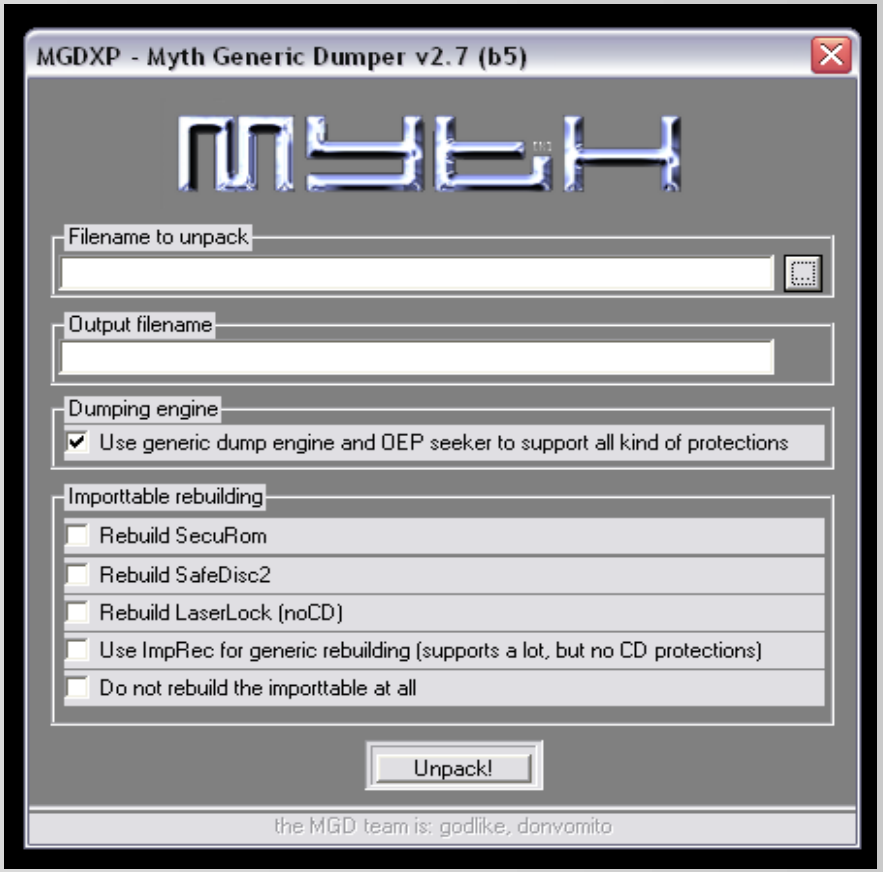
- In order to decide for the right measures against the piracy, it is vital to first learn something about the Scene of Cracking Groups.
- Who are people who remove the copy protection and thus make pirating our games possible in the first place?
- We need to understand their motives, how they work and how they are organized.
- First, let us take a look at how cracked games are distributed world wide between these groups before they reach the general public.

The „Scene“
Know Your Enemy

- Typical life cycle of a game in the pirate scene
  - Game supply: store pickup, distribution pickup, reviewer copy. Watch out for suppliers in your organization!
  - Normal case: Supplier gives .EXE to Cracker, gets cracked .EXE back (<30 min).
  - Supplier generates remastered ISO-Image (inclusively crack), uploads to group internal FTP-Sites (<60 min).
  - ISO gets distributed to all private FTP sites of all other pirate groups world-wide. Mostly, members who are Sys Admins of Universities and ISPs are doing that (<120 min).
  - Non-Sceners with private FTP-Access distribute ISO further and begin P2P sharing (<1 Day).
  - Exponential spreading in P2P networks, Usenet, upload of crack patch on websites like gamecopyworld.com (>1 Day).

The „Scene“
Know Your Enemy

Automatic Cracking Tools

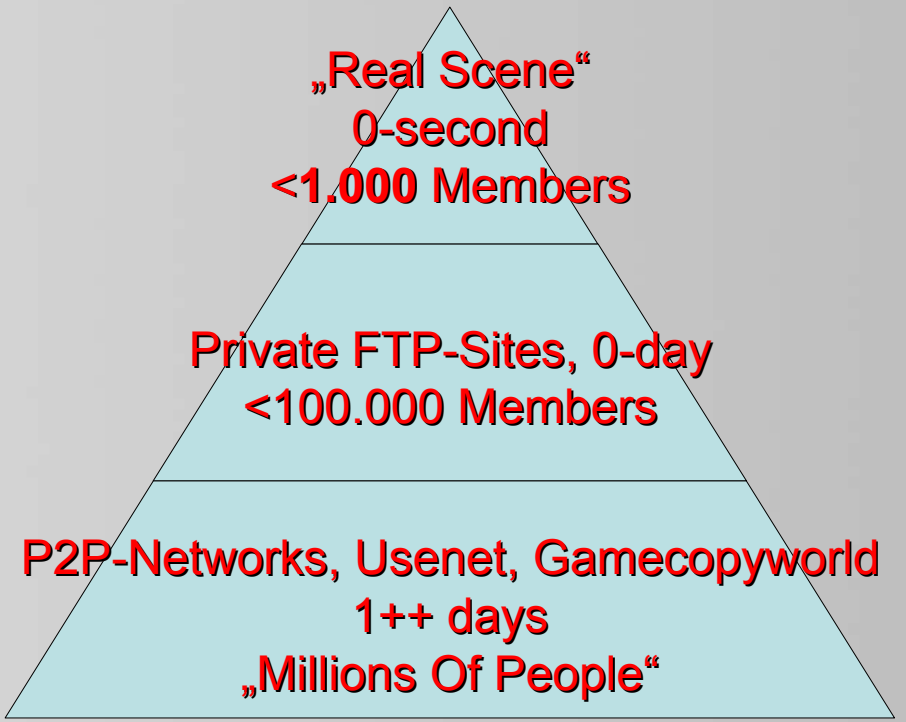


- For all generic protection systems (eg. Safedisc, SecuROM, Laserlok, VOB, StarForce) without added custom code there are generic cracking tools.
- A cracker only needs to change these tools when a protection vendor updates his system significantly (normally many month between versions).
- Non-programmers can easily use these tools.
- Nearly all protection systems can be removed in minutes by these tools.

The „Scene“
Motivation

- Nearly no members of the „Real Scene“ have a commercial motivation.
- Their driving force is the race against other cracking groups for the fastest release of a 100% working crack.
- Most Scene members disapprove of the distribution of cracks and complete versions on websites and P2P-networks (but they carry on cracking, of course).
- That’s why they don’t see developers and distributors as their enemy.
- However, commercial product pirates who facsimile boxes, CDs and manuals use the “work” of the cracking groups for their products.
- Sometimes, product pirates supply online infrastructure to the Scene. This way, they get immediate access to Scene releases.

The „Scene“
Hierarchy



The „Scene“
Summary

- The Scene is well organized and uses all Internet services for their activities. Groups normalyy have members from many regions of the world.
- Crack patches and complete versions are distributed all over the world in a matter of hours.
- There are crackers out there, whose programming and disassembling skills are downright scary. They successfully attack sophisticated obfuscation code at machine code level using powerful disassembly tools.
- But: despite the world-wide network of cracking groups there are not awfully many cracker . The number of highly talented crackers who can attack new protection code lies around 12 Persons world-wide.
  Additionally, there are “retired” Crackers who might react to a call for help and programmers with a Cracker’s skillset who are not Scene members. There are roughly 30 of these.
- This shows that the time budget of even these admittedly very talented crackers can be overloaded under one circumstance:
- There needs to be better protection technology on *more* game releases!

The Goal

- We all know that there is no such thing like an un-crackable copy protection.
- However, with the right amount of effort it is possible to protect the time window in which most of the sales of a game do happen.
- A time frame of about 3-6 weeks without a crack is technically possible.
- If a more publishers decide for a higher protection level of their games, this time frame gets longer automatically because of the Cracker's work overload.

The Vision

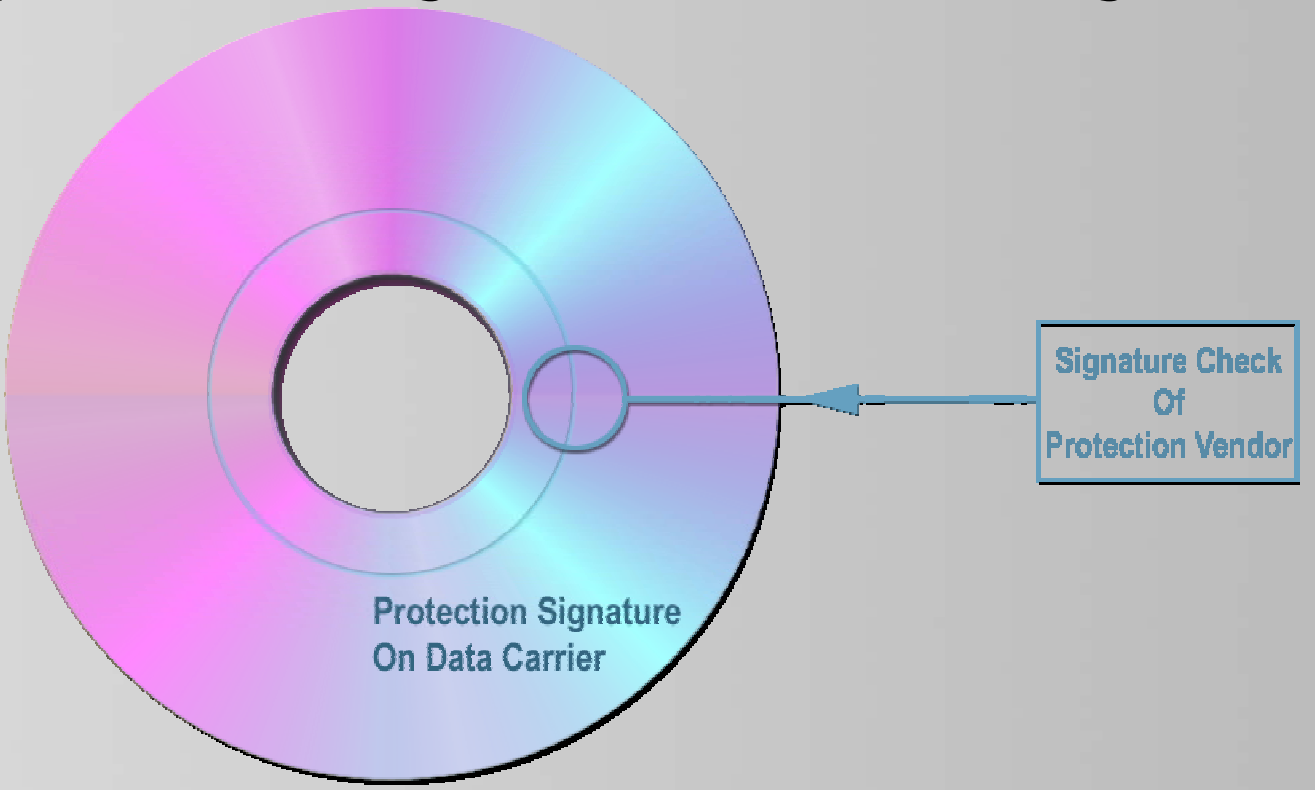
- If all major releases would feature sophisticated protection, there would be a shortage of download alternatives in a given genre.
- People, who are interested in pirate copies, would have to realize that they have to wait for 2 or 3 month before they can download a current title.
- A different way of thinking would be established over time: “When I want to play a new game, I have to buy it.”
- I think that this is not a naïve dream. This vision can be made into a reality if all major publishers would invest a tiny fraction of their development & marketing budgets for the protection of their title.

Principles Of Advanced Copy Protection
Terminology

- **Anti-Reversing, Code Obfuscation**: Code techniques that check for the integrity of copy protection code and make it difficult to alter and remove it.
- **Signature**: physical modification of a data carrier (CD, DVD) that should not be copyable.
- **Signature Check**: Code that validates the authenticity of the signature.

Principles Of Advanced Copy Protection
Basic Structures

- Data carrier based offline protection systems consist of two components; the signature itself and the signature check:



Principles Of Advanced Copy Protection

Basic Structures

- The Signature should be…
  - … not be copyable with even the most current software.
  - … compatible with nearly all CD / DVD drives on the market.
- The Signature Check needs to achieve even more:
  - Simple and fast integration in any software.
  - Should be hard to attack and remove.
  - But should be compatible with all operating system flavors.
  - Should offer a SDK to trigger own signature checks (for repeated checks later in the game).

Principles Of Advanced Copy Protection
Basic Structures

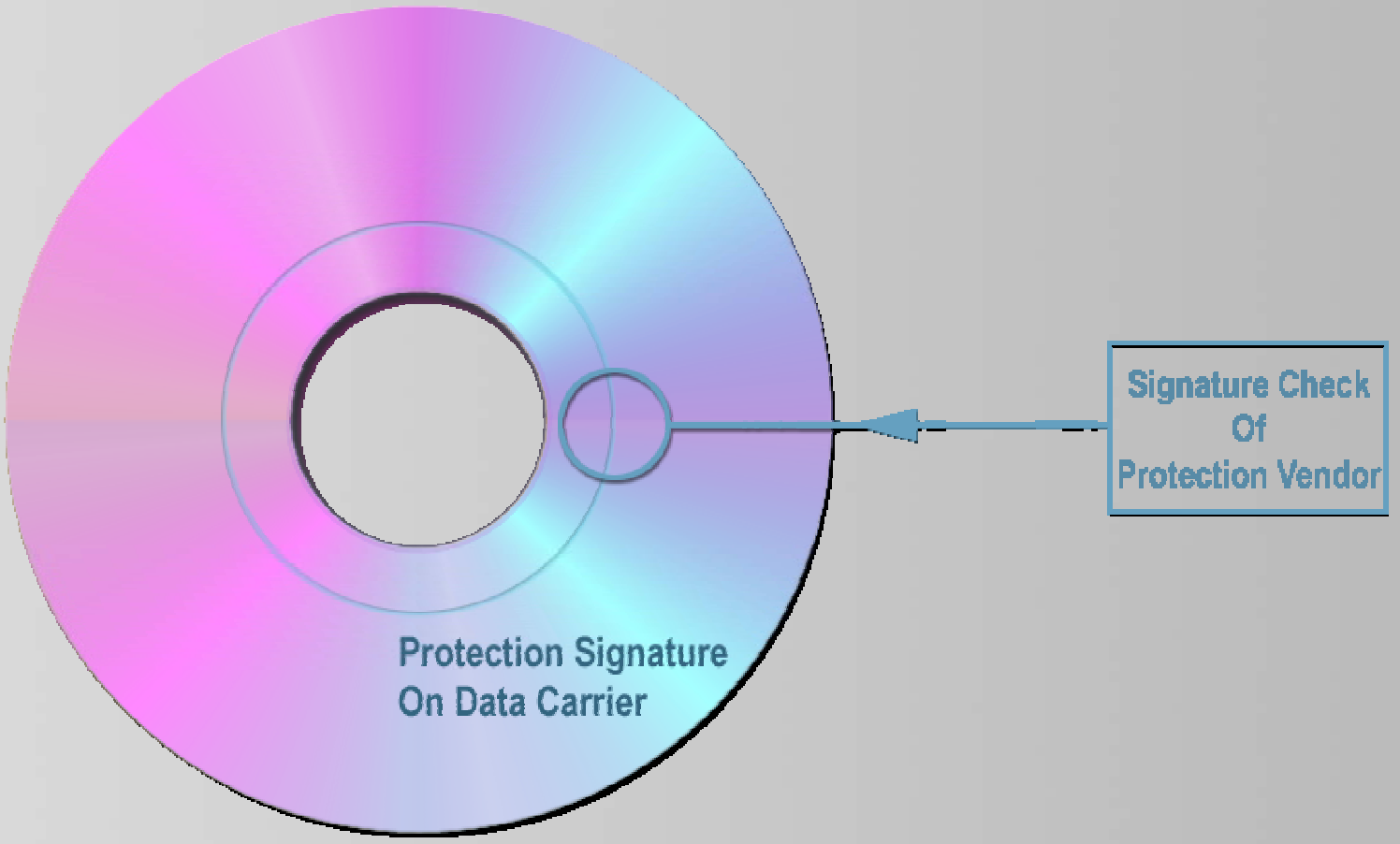
- Beside all methods described in this talk, there is one basic principle that is your most powerful weapon against anyone attacking your code:

- **Custom protection code for every game you release.**

- You definitely don't want to invent your own signature and signature check. You'd end up in compatibility hell.
- The custom protection code always *accompanies* a vendor's proven protection system and cross-checks its integrity.

Principles Of Advanced Copy Protection

Basic Structures

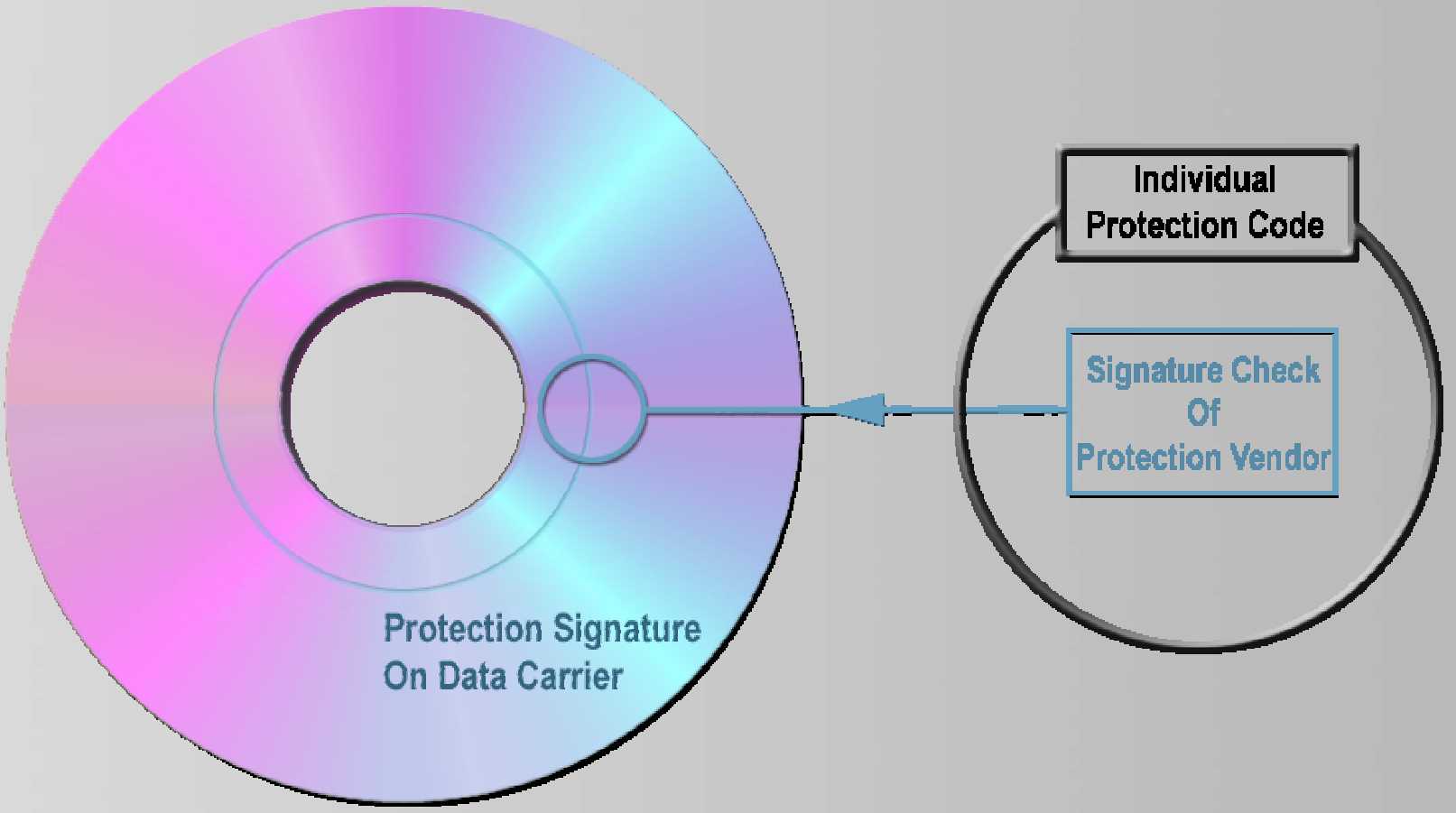


Protected Data Carrier
(1. Component)

Signature Check
(2. Component)

Principles Of Advanced Copy Protection

Basic Structures



Protected Data Carrier
(1. Component)

Signature Check
(2. Component)

Principles Of Advanced Copy Protection
Basic Structures

- Additionally to the technical problems that you want to avoid, it‘s always difficult and time consuming to switch protection vendors or production facilities and to change internal company policies regarding protection issues.
- Therefore, all the following methods can be applied on top of existing protection solutions (although some of them rely on the existence of an SDK to trigger own signature check calls).
- The evaluation of a vendor that offers an effective combination of signature and signature check can be mission critical (more on that later).

Principles Of Advanced Copy Protection
Responsibility Assignments

- Don‘t make the dev team responsible for the development of custom protection technology:
  - Most of the time there’s no-one in the team with the necessary skills.
  - There’s no room in the schedule for tasks like this.
  - It's sufficient to have someone in the team who is responsible as a contact person for the implementation of advanced copy protection code. Ideally, it’s the lead programmer.

Principles Of Advanced Copy Protection

Responsibility Assignments

- There have to be full-time copy protection programmer(s). This group or individual has the following tasks:
  - Continuous evaluation of new copy protection vendors, their signatures and signature check software.
  - Continuous development of anti-reversing code.
  - Evaluation and application of 3rd-party technology like crypting tools.
  - Development of game-integrated check code for the consistency of the protection system.
  - Possibly the modification and implementation of the installer.
  - Keep an eye on the pirate scene and their releases and thus the efficiency of the additional measures.

Principles Of Advanced Copy Protection
Programmer Profile

- The Copy Protection Programmer should have a profile like this:
  - Experienced with reverse engineering and anti - reverse engineering practices.
  - Must know the operating systems, kernels and hardware of the target platforms inside out. PC: expert knowledge of differences between Windows flavors is very important.
  - Good C/C++ skills.
  - Good Assembler skills (doesn't have to be the same person).
  - Experience with common data structures of a game project.
  - Good general knowledge about the cryptography field.
  - Ideally ex-"Scene"-member with hands-on experience in cracking.
- The lead of a copy protection task force should be an experienced game developer. This avoids most potential problems during a game project workflow.

Practical Experiences
Evaluating A Protection Vendor: General Issues

- Assuming that you're planning custom protection enhancements, an SDK for calling signature checks is a basic requirement for buying a protection system.
- Since you're going to integrate your own calls in your game, the most important feature you want to evaluate is the quality of the data carrier signature.
- Important are: copy resistance, compatibility and possible manufacture locations.
- Evaluating the copy resistance of a signature
  - Check postings in boards about CD-burning if a current vendor's signature can be copied and which combination of hardware/software does the job
    - www.cdfreaks.com, support boards of "Alcohol 120%" & "Deamon Tools"
  - Try to make a copy yourself, using the best current hardware/software combination.
  - As with encryption layers and crackers, there's a never-ending race between signatures and CD copy software.
  - Another problem: software that emulates CD drives and protection methods on a users hard disk. Detecting those is very difficult, but possible.

Practical Experiences

Evaluating A Protection Vendor: Compatibility

- Ask vendor for tests he conducted and a list of approved drives.
- Check message boards of games that have been protected by the vendor's system.
- Cost effective in-house tests:
  - Ask vendor for test CD with an immediate response of the protection system (no installation necessary).
  - Make someone responsible for a quick test on all machines and drives in all departments of the company. A list with drive type, hardware and OS version should come out of this.
  - Let your QA department do the same test.
  - Later in the negotiations you might want to let a 3rd party QA company perform a hardware compatibility test.

Practical Experiences

Evaluating A Protection Vendor: Production Plant Location

- Unfortunately, the issue of copy protection is not just a technical one. Many departments of a publishing organization are influenced by it.
- Choosing the right copy protection CD signature can be influenced by current contracts and by the co-operation with distribution partners in international territories, who might want to manufacture CDs by themselves.
- There are basically two kinds of signatures: proprietary solutions of a production plant (e.g. SecuRom by Sony DADC) and independent solutions (e.g. SafeDisc, Starforce, Tages).
- Basically, an independent copy protection signature can be manufactured in every production plant. When such a signature is new for a plant, take into account a potential loss of time by license negotiations and technical issues until the production can start.

Practical Experiences
Developing And Integration Custom Protection

- How creating custom protection code doesn't get into the way of your development teams' schedule:
  - Choose a contact person in the dev team wisely. Should be a coder who's familiar with the whole software architecture of the project. He'll be working closely with the copy protection specialist.
  - All code and methods for securing and cross-checking the integrity of the underlying CD-protection comes from the specialist, only the integration needs to be done by the contact person.
  - Typically, you only need 5 … 10 man-days to integrate a high level custom protection into a project.
- Integrate custom protection between alpha and beta - data structures of the game should be defined then and can be used for additional protection methods (e.g. hiding code segments in big files).
- Got a compiled in-game scripting language? Best way to integrate cross-checks that are hard to find.

Principles Of Advanced Copy Protection Useful Methods

- tbd: 1-2 pages of coding tipps.

Practical Experiences
Developing And Integration Custom Protection

- Of course, the more different cross-checks you use, the more time you'll buy. Just make sure that you keep track of the triggers of the checks and make sure that they can be tested without having to jump through time consuming game play hoops.
- Make sure that all protection code can be enabled and disabled in the build options of your compiler – this way the dev team can decide whether they want to build a protected or unprotected version.
- Testing a protection is surprisingly easy, if you take care that QA has a number of boxes with a second CD drive. This way you can even test gold CDs; the CD with the vendor's signature is in the second drive.
- The above plus a list of copy protection check triggers and failure reactions helps to quickly check if all is well with the protection system in any stage of development.

Practical Experiences
Reactions In Case A Copy Is Detected

- Consider the game's reaction when a copy is detected carefully! There's a conflict here:
- Subtle in-game reactions that mess the game up are extremely hard to find. But owners of illegal copies might flame you for "bugs" in bulletin boards. Examples:
  - Misadjusting balancing parameters make game impossibly hard.
  - Stack, memory and variable manipulations that lead to crashes.
  - Mission critical items vanish.
  - Deactivating important triggers like "mission accomplished".
- But you're opening the code for attacks, when you have an obvious reaction to a check failure like a text message.
- Choose a compromise. The reaction needs to be recognizable at least for the customer support, ideally for the customer, too. Examples:
  - Message like "Please insert game CD" not as text in the code, but as encrypted bitmap graphics.
  - Exit to desktop after clearly defined graphic signals (e.g. messed up lighting).
  - Error messages that sound plausible, but hint to a copy-detected-reaction.
- Give a list of these reaction to customer support before release.

Practical Experiences
Real World Problems

- Integrate early.
  - Otherwise you'll probably end up weakening the protection because people get nervous if something goes wrong with your code in ultra-crunch-mode.
- Keep up a close relation to your copy protection vendor. They appreciate competent feedback and will co-operate with you on new versions of their system.

Practical Experiences
Real World Problems

- Creating sophisticated custom protection code is a really big challenge, but it's manageable if you have the right people on board. But strangely, there seem to be even more problems on the non-technical side.
- Copy protection is an issue that influences the work of all departments of a publisher. There's a lot of misunderstanding about technical issues. Also, collisions with established internal processes and company policies happen. You can be lucky to convince upper management to start a custom protection program at all. And then the trouble just begins…
- To non-technical people, copy protection seems an alluringly easy topic: Program checks CD, you can't copy, all is well. For these group of people it's often hard to understand that you need to take care for a lot of things to avoid sabotaging your companies own efforts.
- My only advice: Explain. And repeat.
- And repeat. And repeat. And repeat. And repeat. And repeat. And repeat. And repeat.
- **And repeat!**
- Some of these problems and some possible solutions follow…

Practical Experiences
Real World Problems

- Unprotected Gold Masters.
  - Gets demanded for archive for later OEM versions.
  - But: internal processes and all people in sales an localization must be aware that unprotected masters never get send to a territory just because they asked for it.
- Unprotected Review-Code.
  - When an important magazines' deadline nears, PR has to know (under the threat of death penalty) that they my not send out unprotected gold CDs.
  - Help PR by creating an automatic fingerprinting tool, so even a non-tech person can generate fingerprinted copies. Some CD burning tools offer command line interfaces for this. (But even so, this should only be used for beta code, not for gold master code).

Practical Experiences
Real World Problems

- No unprotected OEM-Versions during full-price sale period.
  - Would act as crack. Offer shortened OEM version.
- Manufacturing in foreign territories and demands for a different protection.
  - Motivated by cutting down manufacturing cost.
  - Disproportional efforts, may also lead to multiplayer problems because multiplayer part checks for the equal code level.
  - Again: explain & repeat.
- Territorial release delays should be avoided. Copy protection methods have, well, a half-life in their effectiveness. There will be a crack released in no time, if a game was available for several week in another territory.
  - If unavoidable, a modification of the custom protection code might make sense in important territories (watch out for multiplayer & patching problems).

Conclusion: Why Not Going All The Way?

- The biggest problem, however, when it comes to a strong copy protection seems to be recognizing the necessity for it in the first place.
- I'm puzzled that the big publishers still seem to have hesitations against a strong, professionally done copy protection.
  - Strangely, nearly all (PC) games *do* feature a standard protection, thus risking the downsides of protection (rare incompatibilities) while gaining nothing (cracks are available simultaneous to release).
- The reasons are, for me, not really clear.
  - Most bigger companies have IP departments that persecute IP infringements, web piracy and product piracy.
  - They also watch the web and P2P-networks and gather data about the circulation of pirated copies of their games.
  - These data show that piracy is a problem in *all* territories, also in the US. Yet there seems to be no action that results in development efforts.

Conclusion: Why Not Going All The Way?

- Yes, protection technology that withstands attacks for several weeks is a difficult issue. But like no other software area, the game industry is famous for finding solutions for technical challenges!
  - Is it easy to write a 3D engine that runs on all configurations and systems? Of course not, but we manage to do so anyway.
- Compared to our current and future game development budgets, the cost of a dedicated development department for copy protection is minimal. I dare say that **we have so far not seriously taken up the coding fight with crackers and the pirate scene!**
- If we dedicate *serious* resources to it, we will be able to raise the bars of copy protection methods dramatically.
  - Software is easier attacked than defended by principle. Still, like with anything else: When a professional organization invests *serious* efforts into an issue, it's not possible for individual hobbyists to match them.

Conclusion: Why Not Going All The Way?

- The realistic goal is to create copy protection code that withstands attacks for several weeks and runs smoothly on all customers' systems. The key element for that is individual protection code for every project, done by experienced people.
- What's more, our business model is one of the few ones where advanced copy protection actually makes sense. Nearly all of our titles sell the majority of units in the first couple of weeks. Protecting this time frame is a realistic goal.
- Increasing the general copy protection level will benefit the whole industry. It's a self-boosting process: the more anticipated titles are well-protected, the more overloaded the pirate scene will get.
- Another significant gain in sales will take place, when *all* AAA-games feature serious protection, because people interested in pirate copies will have no alternatives in their favorite genres.
- To make all this a reality, the first step has to be done by the leading executives of a company. They have to set not only the goals for the developers, but must also set up supporting structures in the other departments of the organization.

Thank You

For any questions about the realization of this talk's topics you can reach me at my private mail address below.

Erik Simon

erik_simon@gmx.de