

Secure Video Processor

Zen and the Art of Content Protection

An introduction to Content
Protection

March 28, 2004

© SVP 2004. All rights reserved.

This document and the information contained in it is confidential and the property of SVP. The technologies herein may be the subject of patents pending and granted or other similar protection. This document must not be used for commercial purposes other than your own internal discussions nor copied, disclosed, reproduced, stored in a retrieval system or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise), whether in whole or in part without the prior written agreement of SVP. SVP reserves the right to request the return of this document at any time and any copies thereto.

Zen and the Art of Content Protection

An introduction to Content Protection

Table of Contents

1.	THE PROPER MINDSET	1
2.	HOW DIGITAL CONTENT GETS DELIVERED TO THE VIEWER	2
2.1.	STAGE1: UNCOMPRESSED, CLEAR ANALOG OR DIGITAL CONTENT	2
2.2.	STAGE 2: COMPRESSED, CLEAR DIGITAL CONTENT	2
2.3.	STAGE 3: COMPRESSED, SCRAMBLED DIGITAL CONTENT	2
2.4.	STAGE 4: CONTENT DISTRIBUTION.....	2
2.5.	STAGE 5: FROM SCRAMBLED, COMPRESSED DIGITAL CONTENT TO ANALOG CONTENT	3
3.	LEARNING THE HARD WAY.....	4
3.1.	THE FIRST NATIONAL BANK OF HEAVY OBJECTS	4
3.2.	THE SECOND NATIONAL BANK OF THE SECRET TREASURE MAP	5
3.3.	THE THIRD NATIONAL BANK OF IDS	5
3.4.	THE FOUR FOUNDATIONS OF CONTENT PROTECTION	6

1. The Proper Mindset

Acres of trees have been sacrificed on the altar of *content protection*. Vast multitudes of committees, forums and standard bodies have spent light-years of hours debating the pros and cons of 5C, tamper resistant software, triple DES, x509 certificates, etc., etc., etc. Despite these efforts, we have seen the music industry virtually destroyed by Napster and Morpheus. It takes millions of dollars and hundreds of people to create a single movie only to discover that, when the movie is released on DVD, any 14-year-old child equipped with a mid-range PC and a broadband connection, can download software like SmartRipper and, within fifteen minutes, begin distributing high quality free copies of that DVD to the entire world.

If you are looking for a white paper discussing detailed mathematical functions, explaining the cryptographic features and benefits of *blowfish*, or comparing various Zero Knowledge Authentication schemes, you can stop reading now.

This white paper takes a slightly different route. It steps back a level, and tries to see the forest, and not just the trees. Our path starts with a short description of how digital content distribution works in order to understand why some previous attempts at secure distribution have failed. The path concludes with four *foundations of secure content distribution*.

2. How Digital Content Gets Delivered to the Viewer

2.1. Stage 1: uncompressed, clear analog or digital content

The original form is very high quality clear, unencrypted analog or digital content. This is normally called the *master* copy, and is accompanied by a very high level of physical protection. That is, it is protected in locked rooms behind the walls of studios with limited access.

2.2. Stage 2: compressed, clear digital content

It is a basic truth that as an object gets smaller it gets cheaper, easier to send from one location to another. Due to the limitations of the human eye and the power of our brain, it is possible to eliminate major sections from a movie, and we will still observe the same quality as before. In this form, the content is most vulnerable because its size has been significantly reduced, it is easy to distribute, and access is not limited. Therefore, content never stays in this form for very long and it quickly moves to the next stage.

2.3. Stage 3: compressed, scrambled digital content

In this stage, a digital key is generated and the valuable content is scrambled based on the digital key. There are many types of encryption algorithms; DES, AES, 3xDES, Blowfish and others. Certificate, control word, and encryption key are all common names for digital keys.

2.4. Stage 4: content distribution

The next stage is content distribution. The locked content has to get from the content creation location to the viewers. Secure content distribution has one very important feature: each copy of the content has to be paid for. This implies that it must be very difficult to purchase content, and then copy it multiple times.

2.5. Stage 5: from scrambled, compressed digital content to analog content

This is the last stage of content distribution. The content goes from its scrambled and compressed digital form to an uncompressed, clear analog form. The sequence signifies a reverse of the creation stages:

- a. The digital scrambled content is matched with the key and sent to a descrambling device. The descrambling device gets two inputs: the scrambled content and the key, and produces a single output: digital compressed clear content.
- b. The digital compressed clear content is decompressed, into digital uncompressed clear
- c. The digital uncompressed clear content is converted into analog clear form for viewing.

3. Learning the Hard Way

To understand: digital content, encryption algorithms, and digital keys, compare it to the following analogy:

- Digital content = your life's savings
- Encryption algorithm = a safe
- Digital key = the key that unlocks the safe

To enjoy and use digital content a listener/viewer needs the following items:

- The digital content
- The digital key
- A content player that supports the following functions:
 - A way to load the content into it
 - A way to load the keys
 - Knowledge of how to use the keys to unlock the safe and get to the content.

We will now describe a few banks. To judge the services provided by these banks, ask yourself a simple question: Would you trust this bank with your life savings?

3.1. The First National Bank of Heavy Objects

This bank uses an unlocked filing cabinet. As a protection mechanism, it ties a heavy brick to your money to make it hard to carry away. The bank has a big sign that says: "It is against the law to steal money from this bank". As an additional protection mechanism, the bank has recently run advertisements stating that it is against the law to steal from the bank.

The distribution format of CD music uses this model. There is no encryption algorithm. The brick that makes it hard to transport the money is the `.wav` format. The scissors used to cut the string tying the brick to the content is a PC that converts the `.wav` formatted content into MP3 format.

Security based on content being difficult to distribute has a built-in shelf life. Eventually, the forward progress of technology reaches a point where content that was once difficult to distribute is now trivial to distribute.

Note: This will soon become true for analog clear video content as well. That is, it will be trivial to encode and distribute compressed video content.

3.2. The Second National Bank of the Secret Treasure Map

This bank is much more sophisticated than the bank of heavy objects. In this second bank, they store your money in a safe with very thick walls, and then lock the safe with a strong lock and key. To make it easy for people to match up content and keys, the bank decided to hang the key right on the wall of the safe. This makes it very simple to match the locked safe with the right key, since the key hangs right on the wall.

The bank realized that simply hanging the key on the safe was not such a good idea, and that it defeated the purpose of locking the safe in the first place. They had a bright idea to hide the key on the wall of the safe. The concept was to hide the key so that it would be impossible to find without a map and to make the map secret. They buried the treasure map in the ground under the safe. Due to business reasons, the bank worked in two different locations. In the first location, the ground was heavy granite, and it was very hard to dig into the hard rock under the safe to find the map. In the second location, due to geographic constraints, they had to hide the map in the sand.

While this might seem at first to be a good solution, it has major drawbacks. Once someone publishes the treasure map, the entire security system falls apart. To open the safe is very simple: follow the map, find the key, and unlock the safe.

This is how DVDs are distributed. DVDs are encrypted with a strong algorithm and they use a reasonable size digital key, but they distribute the key and the content on the same media.

The DVD player has to be able find the digital key to play the content. Since a single player has to be able to play all DVDs, each DVD has the same map. History shows that trying to hide a secret in PC software is virtually impossible. PC-based DVD players were easily cracked and the secret map was published.

Security based on fixed secrets also has a shelf life. Eventually, technology progresses to a state where it is easy to find the secret. Once the secret is found, the system falls apart. Fixed security elements are impossible to replace.

It is virtually impossible to hide secrets in PC software, since the very nature and design of PCs and PC operating systems makes it almost impossible to have secure PC software.

3.3. The Third National Bank of IDS

This bank learned from the bad experience of using secret treasure maps. Like the second bank, they store your money in a safe with very thick walls, and then lock the safe with a strong lock and key. But instead of attempting to hide the key on the safe, they keep the keys in the basement of the bank. Customers can only get a key after they show an ID card. To enhance security, the bank makes it

impossible for anyone but the bank to issue new ID cards. So far, this seems like a great bank. In our physical world this bank would work.

However, the bank suffers from a very poor geographical location: it is located on a planet where everyone has the exact same face and fingerprints. The bank also does not prevent its customers from making copies of their ID cards. The bank soon found that a single ID card was being copied again and again. Since everyone looked the same, it was almost impossible to check if the ID card had been issued to the person who was now presenting it. The bank soon discovered that it was giving out keys to the wrong people, and that ID cards on a planet where people all look the same do not really work well at all.

This is what is happening to the secure distribution of electronic content to PCs based on certificates. The main reason secure distribution based on certificates fails is that it is trivial to copy a certificate and send it to any PC. Since, by its very design, the PC is a ubiquitous device, it is virtually impossible to establish its unique identity, and create a certificate that will only work on one PC and not on millions of other devices.

3.4. The four foundations of content protection

Following are the four foundations of content protection upon which SVP builds its content protection systems.

1. Content should be encrypted until the last possible moment prior to viewing by following these steps:
 - a. Never distribute content in the clear
 - b. Never allow devices to store content in the clear
 - c. Keep all content scrambled until the last possible moment when it needs to be displayed for viewing
2. Controlling the keys is just as important as scrambling the content.
 - a. Never distribute the keys with the content.
 - b. Make it very difficult to create a key.
 - c. Make it difficult to copy a key.
 - d. Store all keys in a renewable secure key storage location.
 - e. Make sure that each renewable secure key storage location has a unique ID that is hard to copy and hard to fake.
3. When playing scrambled content follow these steps:

- a. Load the scrambled content
 - b. Before accessing a secure key storage location, verify that it is legitimate (*i.e., authenticate it*), and has not been tampered with and is still valid (*i.e., has not been revoked*).
 - c. Set up a private communication link between the authenticated, renewable secure key storage location and the playing device.
 - d. It is preferable that steps 3.b and 3.c are performed in the same chip.
 - e. Perform all of Stage 5 (see section 2.5., page 3) in a single step.
 - Never allow access to the content between Stage 5a, and 5b.
 - Never allow software to access content between Stage 5b and 5c.
4. Content players fall into two groups, and require separate distribution policies.
- a. Class A: Devices that perform all of stage 5 in hardware are dedicated players.
 - b. Class B: Devices that perform parts of stage five in software are PCs.

Note: Devices in this category do not comply with security foundation 3.d and are therefore inherently much less secure.

Therefore, use the following distribution policy:

- Ensure that content is paid for and released on Class A devices **before** it is available for use on Class B devices.
- Ensure that content released for a Class A device is cannot be used on a Class B device. In other words, design the Class A device with a content distribution format that does not work on Class B devices. *{This is not that difficult to do. As an example, try using a Sony Playstation CD on a PC. The gaming industry uses this foundation. Each type of device uses a different format}*

To ensure distribution security over a long period of time, each of these four foundations must be implemented.