USENIX
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

The following paper was originally published in the

*USENIX Workshop on Smartcard Technology*

Chicago, Illinois, USA, May 10–11, 1999

# Beyond Cryptographic Conditional Access

*David M. Goldschlag and David W. Kravitz*
*Divx*



For more information about the USENIX Association:
Phone: 1 510 528 8649 FAX: 1 510 548 5738
Email: office@usenix.org WWW: http://www.usenix.org

# Beyond Cryptographic Conditional Access

David M. Goldschlag
David W. Kravitz
*Divx*
*570 Herndon Parkway*
*Herndon, VA 20170, USA*

## Abstract

Conditional access (CA) systems manage chargeable content (e.g., movies). Traditional CA systems use a smartcard as a cryptographic component that decrypts broadcast content for authorized recipients. Since that approach protects content by protecting cryptographic keys, it has two inherent weaknesses: It relies on the smartcard to protect universal secrets (i.e., the broadcast keys); and it cannot protect content from redistribution. This paper describes a non-cryptographic conditional access system, where instead of protecting content directly, the content's identity is inserted as a watermark in the content and the CA smartcard is used as a licensing authority to authorize the display device to display watermarked content. This approach places a lower security burden on individual smartcards, and protects against the use of redistributed content.

Keywords: Authentication, authorization, conditional access, copyright protection, licensing, smart cards, trust management, watermarking.

## 1. Introduction

Conditional access (CA) systems control access to chargeable content. This content includes both data and entertainment products such as movies or music. The content may be delivered in many ways, including broadcast from satellite or a local broadcaster, transmitted over cable or the Internet, or delivered by fixed media, such as a DVD. Billing policies also vary greatly: content may be sold as part of a subscription such as premium movie channels, by the unit like pay-per-view movies, or incrementally as in a stock ticker that is charged by access time.

Traditional CA systems protect chargeable content cryptographically. The primary function of a CA system is to report content access to a billing system, and to prevent unreported access to content. To force content to be accessed through the CA system, content may be encrypted using cryptographic keys known only by the CA system. In that model, encrypted content is broadcast by a headend system and accessed through a CA smartcard on the user's set-top-box (STB, e.g., a TV or cable tuner). Accesses are reported to a backend billing system. The distribution of content keys is managed by a key management system (KMS) that lets CA smartcards learn the keys needed to decrypt content.

Cryptographic CA systems require the CA smartcard to protect content keys. Since efficient broadcasting requires universal shared secrets (i.e., there is a single broadcast data stream for any content), each smartcard must be trusted to protect universal secrets. This is a severe security burden for the smartcard. The pirate may use significant resources to compromise a single smartcard, and learn the keys necessary to decrypt content. Those keys are useful to all recipients of the content. Furthermore, CA systems are attempting to solve an inherent paradox: How is access to content enabled yet still controlled? The STB must have access to the unencrypted content. The pirate may attack his STB, obtain the content, and redistribute it. This threat has typically been called copy protection, and is not a CA threat, as long as redistribution is expensive.

We are concerned about CA in an environment where redistribution and storage of content and keys is cheap. Although this is not yet true for high quality video, it will be true, and it is appropriate to design systems that are resistant to this threat. Notice that display devices will always have to display free video, at least from camcorders. So the pirate can redistribute a pirated movie as a home video.

Our proposed architecture uses the CA smartcard as a licensing authority, instead of a decryption device. When granting authorization, a CA device may also log content access, so the access may be billed for.

If display devices required authorization to display certain content, and would refuse to display the content in the absence of appropriate authorization, content would be secure independently of how it was delivered to the display device. The assumption here is that display devices like monitors are expensive and difficult to manufacture and service, and that pirates will not be able to compete in that market.

In this architecture, instead of protecting against the copying and redistribution of the content, we prevent unauthorized access to the content. This architecture places the security where it belongs, at the customer of the pirate, who will be unwilling to spend significant resources to defeat the system. In contrast, in cryptographic copy protection, the pirate can leverage off of his investment, without requiring further investment by the consumer.

This paper is organized in the following way: Section 2 presents an overview of traditional CA systems. Section 3 presents the non-cryptographic CA architecture. Section 4 describes related work. Section 5 presents some concluding remarks.

## 2. Cryptographic CA Overview

A model of a CA system is illustrated in Figure 1. Notice that content keys need not be delivered with the content, although they may be, and that the backend billing system may be independent of the headend too.

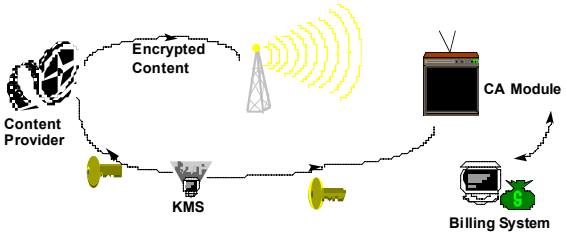


**Figure 1: Model of CA Infrastructure**

The billing system has two security roles: one is to instruct the key management system which keys should be sent to individual CA smartcards, and the other is to upload logs of key use from CA smartcards. These two functions correspond to advance billing for subscription services, and credit-type billing for pay-per-view services (i.e., where services are used before they are paid for).

The CA smartcard, which is present in every user's house, must protect cryptographic keys that are universally useful. That is, the keys that a CA smartcard uses to decrypt content are equally useful to other recipients of the broadcast. If those keys are compromised and distributed, other recipients of the broadcast may use the keys to access content for free. In particular, since there is more content than keys (e.g., content takes up more bandwidth than keys), a pirate can leverage off of the original broadcast, only redistribute keys, and make money at the broadcaster's expense.

In cryptographic CA systems, the CA smartcard is a hardware device that protects keys. The security of this hardware decreases over time, because its design flaws become known, and physical attacks against it become cheaper. Furthermore, the pirate may be able to amortize the cost of attacking a single smartcard over the sale of many counterfeit smartcard. This suggests that the CA smartcard be renewable, so the security of the CA infrastructure may evolve over time. The challenge is to design an infrastructure that admits increasing security at low cost over a long lifetime.

## 3. Non-Cryptographic Conditional Access

If content redistribution is easy, there is no real point in protecting content up front, by encryption, for example. Imagine that bandwidth was very cheap: HBO may have a single customer, a pirate, who redistributes content to everyone else. Service providers cannot sustain businesses in such an environment. In this section, we describe a possible direction for protecting content in such a threat environment.

Notice that securing the input ports in the playback (display) device is not an adequate solution, since customers must always be able to play home-generated content (like output from a camcorder) and the pirate could redistribute content as if it were generated by a camcorder. We must prevent chargeable content from masquerading as free content. Even if in the future, camcorders would mark their content in such a way that chargeable content would

not carry the free-content markings, this alone would not address the playing of legacy content generated by existing camcorders because a pirate could redistribute new chargeable content in the old home-generated content (unmarked) form.

The current reality of smartcard technology forces us to acknowledge that CA smartcards are not completely impervious to compromise. This together with the fact that at some point the plaintext content data is routed through the non-renewable playback device, forces us to focus on preventing successful use of the pirated content by potential customers of the pirate, rather than on preventing acquisition of the pirated content in the first place if we treat the content redistribution problem as a surmountable impediment. We want to take advantage of the fact that even if the pirate and his customers want to consider the use of pirate-provided non-compliant playback devices, the sophisticated monitor technology in display devices imposes significant barriers to entry for small- to mid- scale piracy operations.

Assume that the analog content itself can be watermarked in some robust way at authoring time, so legitimate playback devices will detect the watermark. Assume furthermore that the pirate cannot remove this watermark without significantly degrading the quality of the viewing experience. Watermark removal is usually done by corrupting the content, or by comparing two instances of the content with different watermarks. This latter attack need not be enabled in this approach, since all instances of the content will have the same watermark (i.e., watermarking is done here for playback control purposes, and not for tracing the source of unauthorized distribution). Unlike "fingerprinting," in this approach the content is watermarked at authoring time.

Assume that each legitimate playback device (i.e., TV monitor) is bound to a limited set of CA smartcards, so that it will refuse to accept critical commands from any smartcard which cannot authenticate these commands as being generated by a smartcard in the distinguished set. A playback device may be bound to a smartcard by receiving a binding certificate signed by a recognized binding authority that binds the playback device to the smartcard. The binding certificate gives the playback device permission to trust responses from the specified smartcard. The playback device need not be authenticated to the smartcard: That is, the smartcard will sign authorization requests from any playback device.

Notice that this binding between a playback device and a smartcard need not rely on the playback device having an externally discernible identity. For example, the playback device may issue a randomly generated bit-string, where the concatenation of this bit-string with the public key of a smartcard with which the playback device is allowed to communicate, is signed by the recognized binding authority.

To play watermarked content, each legitimate playback device requires authorization from the CA smartcard each time it encounters an embedded watermark signal which differs from the one just previous. At the onset of attempted content play, the first embedded watermark signal always results in an authorization request. If this compression of challenges based on limiting authentication requests to deltas in the embedded signals proves to be ineffective when processing content because changes occur too frequently, either the authorization device or the display device may go into alarm condition. The authoring process must embed the watermark signals with sufficient frequency so as to satisfy the most demanding playback devices.

Even if there is no change in the embedded watermarks detected by the playback device, after a certain amount of viewing as determined by the appropriate metric of say, time or footage, the playback device may require an authorization from the CA smartcard if play is to continue. The CA smartcard does not need to process or even receive the entire content stream, but rather only the embedded information from the watermarked snippets the display device detects. So instead of decrypting content for the TV monitor, the CA smartcard becomes an authorized licensing device. The legitimate playback device inspects content to see if a playback license is required, and the playback device refuses to play marked content if no license is presented.

The watermarking of the content done during authoring may be done without regard to the billing infrastructure as long as the embedded signals differ across content so as to allow proper granularity when reconciling the billing process. If every title is marked distinctly, this will allow for later arbitrary assignments of billing units.

Freshness considerations must be addressed so that presentation of licenses or authorizations by the CA smartcard cannot be effectively replayed so as to circumvent appropriate billing for multiple viewings of the same content. For example, the playback

device may include a random number along with the watermark in the authorization request..

Compromise of this system requires the pirate to corrupt the watermark while still maintaining product quality, or produce playback devices that ignore the watermark, or compromise individual customers' CA smartcards. This should be considered an evolutionary approach to security, in that as watermark technology improves, new chargeable content can be released with the newest watermarks embedded as well as with the more vulnerable previous types of watermarks [9]. This allows for backwards compatibility with a population of display devices which shrinks as a percentage of the customer base of compliant devices as new more fully-featured display devices continually enter the marketplace.

The binding authority is essentially a certification authority and many techniques are known for preventing a single source of compromise for signing operations. For example, a hierarchy of signing authorities may exist so the root key is used infrequently [10]. Furthermore, any signing operation may really be the result of multiple signing operations, so the compromise of a single machine does not compromise the combined signature operation [11]. Finally, via signature schemes using "proactive" security, the multiple signing operations must be temporally related, so the compromise of a sufficient number of the individual signing operations must be done within a single window, in order to compromise the signature operation [12].

## 4. Related Work

Watermarks [2,9] carry an embedded signal within the desired signal and have been part of proposed solutions for many forms of copyright control, in particular copy protection. For example, a movie may carry a watermark that instructs a VCR that it is not a recordable signal. The focus of such work has been copy protection and not conditional access.

Watermarks differ from fingerprints [1]. Fingerprints are signals in content that enable tracing information about the particular use or instance of the content (e.g., the name of the purchaser). Fingerprinting must be resistant to collusion, since an attacker may compare and combine different instances of the content. In our application, however, a particular content will have a single signal representing its billing ID.

Linnartz [7], Linnartz, Depovere, Kalker [8], and Epstein [3] also discuss watermarking in the context of copy protection and conditional access.

[8] differentiates between playback control and recording control, where a pirate may disable watermark checking functionality within his own hacked recorder while finding it more difficult to produce content which plays back on standard (i.e., compliant) players. When dealing with the conversion from "one-copy" to "no-more-copy," the authors do not want to provide a hook for hackers to break the system. Their proposal also addresses "never-copy" and "free-copy" (i.e., no watermark) material.

They utilize electronic recognition of the storage medium (ROM vs. RAM), a "physical mark" P embedded on the disc which cannot be read or recovered externally of the drive, and authorization tickets T. One goal is to prohibit playback of "never-copy" content from non-original media. During mastering of the ROM disc, the manufacturer performs the operation P=F(U) where U is a seed provided by (and only known to) the content owner and F is an appropriate one-way function. It is possible to have the construction of P from U designate specific publishers through appropriate design of the function F. It is intended that the physical mark reserved for ROM content is hard for a casual copier to insert on RAM discs.

It is claimed that a pirate publisher attempting to write a particular P in order to make a bit-exact copy of a copyrighted disc must tamper with the DVD press (which he may not own) if the press expects to be given the value of U which is not known to the pirate. According to Linnartz [7], one realization of such a physical mark P is the "wobble groove" in optical disks. If a disc contains a P reserved for professional content, and the content contains a watermark W, then playback requires that: W=F(P) is satisfied in the case of never-copy; that the validation ticket T is present and that T=F(P) and W=F(F(F(T))) are satisfied (where F(T) replaces T at the output of the drive) in the case of one-copy; that W=F(T) is satisfied in the case of no-more-copy. Playback is also allowed if the disc contains a physical mark reserved for recordable media and the content contains a valid W which is used for professional recording and the validated one-copy T is pre-

sent and W=F(T). During recording, the compliant recorder passes the ticket through the one-way function F before transferring it to disc. Recording of copyrighted content is allowed only if W=F(F(T)).

## 5. Conclusion

This paper presented a non-cryptographic CA system that protects content both against conditional access (initial purchase) threats, and copy protection (redistribution or repeated access) threats. The CA smartcard functions as a license authority that is able to authorize display devices to display protected content. Since the display device will only accept authorizations from the paired CA smartcard, the pirate cannot build a counterfeit licensing authority based on his smartcard and sell it to his customers [4,6]. These CA smartcards need not contain universal (system-wide) secrets, making them less attractive security targets.

The efficacy of this system depends upon both the robustness of watermarking and the prevalence and robustness of display devices that detect watermarks and require authorization. How can this detection and authorization capability become standard in display devices? One technique is for it to be bundled with licensed technology that is a desirable feature or to make it part of a being a compliant product (e.g., in DVD systems, CSS security is part of the DVD specification).

## Acknowledgments

This paper benefited greatly from discussions with Michael Epstein and from the comments of the anonymous referees.

## References

1. D. Boneh, and J. Shaw. "Collusion-secure Fingerprinting for Digital Data," Advances in Cryptology: Proceedings, CRYPTO '95, Springer-Verlag, 1995.

2. I.J. Cox, J. Kilian, T. Leighton, and T. Shamoon. "A Secure Robust Watermark for Multimedia," Workshop on Information Hiding, University of Cambridge, Springer-Verlag, 1996.

3. M. Epstein. "The Use of Watermarking to Protect High Value Watermarking Material," ATSC, 7/22/98.

4. 'Open Verifier' Functionality in Consumer Electronics Devices, GD-T204, Release B, News Data Systems, Ltd.

5. ISO 7816 Identification Cards, Integrated Circuit Cards with Contact, 1987.

6. D.M. Goldschlag and D.W. Kravitz. "Pirate Card Rejection," Cardis 98, Louvain-la-Nueve, Belgium, September 14-16, 1998.

7. J.P.M.G. Linnartz. "The 'Ticket" Concept for Copy Control Based on Embedded Signalling," ESORICS 98, Louvain-la-Nueve, Belgium, September 16-18, 1998.

8. J.P. Linnartz, G. Depovere, and T. Kalker. "Philips Electronics Response to Call for Proposals Issued by the Data Hiding Subgroup Copy Protection Technical Working Group," July 1997.

9. F.A.P. Petitcolas, R. J. Anderson, and M.G. Kuhn. "Attacks on Copyright Marking Systems," Second Workshop on Information Hiding, Portland, Oregon, LNCS 1525, pages 218-238, Springer-Verlag, April, 1998.

10. CCITT, Recommendation X.509, "The Directory-authentication Framework," Consultation Committee, International Telephone and Telegraph, International Telecommunications Union, Geneva, 1989.

11. C. Boyd, "Digital Multisignatures," IMA Conference on Cryptography and Coding, Claredon Press, pages 241-246, (Eds. H. Baker and F. Piper), 1986.

12. A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, M. Yung, "Proactive Public-Key and Signature Schemes," The 4th ACM Symposium on Computer and Communications Security, April, 1997.