CONDITIONAL ACCESS FOR COMPRESSION SYSTEMS: DESIRABLE ATTRIBUTES AND SELECTION CRITERIA

Graham S. Stubbs
Graham Stubbs Associates

Abstract

During the next few years, cable systems will apply digitally compressed video technology to provide a vastly expanded selection of programs and services to subscribers. The cable industry has a unique opportunity to apply fresh thinking to requirements for conditional access and security in the digital era, having lived for almost a decade and a half with addressability applied to analog signals.

This paper discusses the process and criteria by which alternative conditional access methods and architectures can be evaluated, and suggests desirable key attributes and features. The industry should not place on its systems/hardware suppliers the entire burden of assuring security, functionality and compatibility. A fresh approach to permit system operators and programmers to thoroughly evaluate security, in particular, should be an essential part of the process.

INTRODUCTION

As the cable industry moves to 500-plus channels of digitally compressed programming, the requirements for conditional access will evolve far beyond the tiered addressability presently in use. A new generation will be required of subscriber equipment, and new thinking about control methodology, compatibility, and security to protect services of ever increasing value. The introduction of the new technology also provides the opportunity to address conditional-access issues in a co-ordinated way, and to seek industry consensus on some of the major factors.

Just because digital compression employs exciting new technology is no reason to be complacent about making sure that its implementation is directed properly. The involvement of the industry's major suppliers doesn't preclude firm direction from the operators and programmers whose businesses will be dependent upon successful operation of the technology. Experience with satellite scrambling and cable addressability should teach us that there is much to be gained by planning ahead.

- Widespread theft of satellite delivered programming has taught that encryption of digital (audio) signals is not automatic proof against piracy - secure handling of the authorization process is key.

- The functionality of cable addressable systems has always seemed to involve a struggle to catch up with market needs - there never seems to be quite enough tags/tiers to deal with the latest PPV offering.

- Addressable converter-descramblers brought in new ways to market cable services and to create additional value - but along came a new set of compatibility issues.

Digital compression brings with it the possibility and promise of a major improvement in security. In principle, encryption of a digital data stream can be

much more secure than scrambling of an analog video signal - but only if the authorization system is designed properly. **Encrypted digital compression does not automatically equate to highly secure.** Similarly the introduction of an all new compressed delivery system will not automatically equate to the functionality appropriate to deliver new services and with compatible operation with TV receivers and VCR's.

An initiative must be taken by the cable's operators and programmers to set out clear requirements for security, functionality and compatibility. It may be useful to refer to the Advanced Television Systems Committee (ATSC) conducted study of desirable attributes and features of conditional access for high definition television (ref 1). ATSC created a list of attributes and features for the guidance of ATV proponents, and to be used as a checklist in evaluating conditional access aspects of proposed systems. Similarly, the development of conditional access requirements for digital compression systems, soon to be introduced, is essential to assure early introduction of secure products with hoped-for features and compatibility of operation. The development of digitally compressed home terminal will represent very substantial investments in engineering and customized components on the part of the industry's vendors. Resolution of these issues should occur **now**, before the first new products are deployed.

OPPORTUNITY AND INDUSTRY PROCESS

Industry focus on digital compression is driven by a sense of urgency related to competitive threats. Much of the activity has centered on development of compression algorithms and digital transportation layer protocols. At a time when these issues are being resolved, the industry has an opportunity for a thorough examination of security, functionality and compatibility issues associated with conditional access.

For many years, proprietary (and largely incompatible) scrambling designs have dominated the marketing of addressable set top cable converter equipment - somewhat to the cost and disadvantage of operators. When digital compression systems are introduced, there is no reason to allow this to recur. It should be possible to develop a commonality of approach which will allow for multiple vendors, and yet assure operators of system level control over security.

At some point in time it may be possible and appropriate to build some portion of the digital channel selection, decompression and control functions into TV receivers and VCR's. Such an evolution will require development of standardized interface specifications, leaving replaceable, critical control elements still at the discretion of operators and programmers.

Possibly sooner than many of us have thought, the compression system will also serve as a platform for the delivery of computer services requiring high bandwidths; indeed the national cable infrastructure is probably the ideal vehicle for driving computer networking at the consumer level.

What is proposed is a co-ordinated industry effort to establish requirements for conditional access in the areas of:

- **security**
- **functionality**
- **compatibility**

A comprehensive listing of desirable attributes and features for each of these aspects of conditional access should be developed, together with a methodology for evaluation. The work should be spearheaded by cable system operators and

programmers whose services will be delivered and controlled by the new generation of digital equipment.

SETTING GOALS

Security

Conditional access systems, once deployed, will be subject to piracy attempts. Indeed, almost any security technology will have the possibility of being broken at some point in time. The cost of piracy must be made very high in relation to the perceived value of pirated programming and services, and, anticipating that some kind of security breach will eventually occur, the system must be capable of recovering from compromise at minimal cost. To the extent that existing cable and satellite scrambling and encryption systems have been defeated, it has in almost every case been by modification of home terminals (set-top-decoders) already provided for legitimate access to programming; attention to the physical aspects of security will always be important. To the extent that security can ultimately be designed to reside in replaceable components (e.g. smart cards), the industry must be satisfied that the cost of cloning and distributing unauthorized devices is extremely high. It is essential that cable operators retain control of whatever equipment the replaceable element plugs into. It may also be necessary that provision be made for electronic countermeasures to be sent over some alternate physical path such as telephone line.

Security Attributes

- The conditional access system must permit recovery from **any** security compromise.
- Security should be contained entirely in the delivery and processing of encrypted keys.
- Access to any one program or service should not facilitate unauthorized access to any other.
- Provision should be made for local cable system intervention and control of satellite delivered programs.
- Operation must be secure even when the threatening party has total system information.
- The ability should exist to exchange key security components at minimal cost.
- It should be non-feasible to recover clear information or control signals by real-time inspection of the encrypted data stream.
- Subscriber hardware should be physically secure to prevent the replacement of components critical to security with other readily available components. Critical security components (e.g. smart cards) should not be accessible to outside probing.
- The cost of cloned devices or components should be much greater than the deferred service cost.

Functionality Issues

As compared with most analog addressable systems, some of the primary issues affecting functionality for conditional access with digital compression are:

- The much larger numbers and variety of channels/program choices/tiers/ program packages/and other digital services to be controlled. Control of high speed data services for personal computers should also be considered.
- Need for multiple operator/programmer control.

- Provision for interactive program requests.

- Requirements for high speed authorization and deauthorization.

- Control of delivery of encryption keys.

- Logistics of using exchangeable security components such as smart cards.

(Smart cards are certain to be an element of conditional access systems. But smart cards on their own are not the total answer to secure conditional access. Cards must be designed to be totally immune to outside probing - a requirement not to be taken lightly. Program code and data storage memories within smart cards should be encrypted, and any attempt to discover the value of the keys used should result in erasure of the card's contents. Operational security requires a lock-interaction between the smart card and the device into which it is connected. The card should be locked using an algorithm from the first unit into which it is plugged, causing the smart-card to be un-usable in any other unit.)

Compatibility Issues

Bringing 500-plus cable channels into a subscribers home introduces new challenges for the configuration of conditional access terminal equipment. When first introduced (projected to be in 1994), digitally compressed signals will be decompressed and restored to analog NTSC format for connection to existing television receivers and recorders.

Configurations to achieve this will include set-top tuner/decompression boxes, point-of-entry devices, and decompression devices at a node removed from the subscribers premises.

Compatibility provisions of the cable Act of 1993 constitute a serious challenge to the industry's use of analog addressability. Some of the unique characteristics of digitally compressed programming provide both a new set of potential problems, and also an opportunity - with careful planning - to try to "do things right." Rather than a set of suggested attributes, the following are some of the compatibility issues to be confronted.

- Availability of a large number of channels (perhaps greater than 500) is likely to lead to provision of programs at multiple time slots. The process for the subscriber to select a program/time slot is likely to be menu driven, and will not likely resemble channel selection as mostly used today. Universal remote control program selections will likely need to accommodate such new ways of perceiving digital program selection, and additionally, control TVs and VCRs.

- Digitally delivered programming will be almost artifact free (certainly fee of cable system analog distortions such as cross modulation, beats, etc.) Putting the digitally delivered image into a TV screen free from the noise and distortion inherent in TV timers will be a challenge.

- Anticipation of digitally compressed program delivery is bound to affect consideration of solutions to the industry's present issues of compatibility in delivering analog signals. There is, for example, no digital equivalent of clear signal delivery with interdiction. Some form of set-top device is certain to be required for delivery of digitally compressed programming for many years.

- Compatibility with digitally compressed high-definition programs will also be an issue, once a U.S. standard for HDTV is selected.

EVALUATION METHODOLOGY

Evaluation of proposed conditional access technologies should give first priority to security. If security is compromised early, it is difficult and expensive to patch it later.

It is essential that a conditional access technology survive security challenges over the entire life of the technology, meaning more than the expected service life of the subscriber terminal; it is important that security can be assured for as long as the compressed signal format remain in use.

In order to achieve the maximum confidence in security, the process of evaluation and selection of a secure conditional access system should start with the assertion that "this is a decision completely separate from the selection of compression technology (or the selection of compression system vendors)" (ref. 2).

Similarly, the evaluation of functionality and compatibility should be separated from decisions regarding compression algorithms, transport layers, and vendors.

It is important that the evaluation process include independent outside expertise - including individuals and companies with insight into the non-conventional methods favored by signal pirates in the past. The industry's twenty year experience with scrambling and encryption reveals that systems have almost always been circumvented by employing short cuts in ways never imagined by the original system engineers. Security of encryption algorithms or of smart cards is only a part of the equation; total system security is the only thing that ultimately matters. It is also essential to the evaluation process that would-be suppliers provide complete disclosure, including **all** details of systems, the results of their own and independent security analyses, and their own knowledge of potential threats.

CONCLUSION

Conditional access objectives for security functionality and compatibility need to be established **now** by the operators and programmers who will commit their businesses to the use of digital compression technology in coming years. An industry process can and should be initiated to specify desirable features and attributes, and to communicate these requirements to industry vendors. As digital compression systems are proposed by vendors for introduction, the industry needs to be satisfied that security and other goals have been met by independent and exhaustive evaluation.

REFERENCES

1. ATSC Document T3/180, "ATV Conditional Access System Characteristics," rev. Sep. 18, 1992.

2. "Conditional access via digital compression" by Graham Stubbs, Communications Technology, March 1993.

ACKNOWLEDGMENT

The Advanced Television Systems Committee (ATSC) developed and published in 1992 a list of Conditional-Access System Characteristics appropriate to advance television (HDTV) systems. The approach taken in the present paper is based in part upon the work reported by ATSC.