CONDITIONAL ACCESS AND ENCRYPTION OPTIONS FOR DIGITAL COMPRESSION SYSTEMS

TV/COM International
16516 Via Esprillo
San Diego, CA 92127

Tony Wechselberger
Executive Vice President

Abstract

The development of digital transport of television signals marks a change from traditional approaches for "secure" distribution using analog scrambling technology. The all-digital nature of these signals makes hard encryption of all program services and network information possible, and thus our expectations for good security performance over long periods of time in future digital compression systems is high.

At the same time there is much effort today to standardize elements and subsystems of this new technology, such that maximum benefits accrue from interoperability with related developing technologies and markets. This paper discusses the issues surrounding encryption in digital compression systems, and explores the possibilities for encryption standardization in certain areas of the transport level. Included are comments on replaceable "Smart Card" and "Processor Card" approaches and benefits.

INTRODUCTION

The consumer and commercial business and entertainment television industries have now some twenty years of experience in the design, fielding and operation of privacy/conditional access systems. Many methodologies have been developed for terrestrial, satellite and cable distribution for both broadcast and point-to-point applications.

For entertainment distribution, true encryption techniques were introduced in the early 1980's. Since that time there has been a steady increase in the adoption of encryption techniques, leading (eventually) to a better awareness in, and utility of proper application of cryptographic technology.

Except for very high cost systems that could afford total digitization of the audio and video material, virtually all existing systems have employed techniques that use the "randomizing" capabilities of encryption to deterministically "scramble" analog program components, and reorder or otherwise reassemble these components at the receiving end. Examples of this are line shuffling, cut-and-rotation, and random inversion of video.

The fundamentally analog nature of the above randomizing approaches has problems. For example, in most implementations (but not all) enough recognizable information remains in the received programming to sometimes not satisfy desired requirements of a good conditional access security

system—namely that the scrambled information contain no useful remnants of its original form, and that reconstruction of the signal not be possible by examination of the scrambled waveform alone. (For a good treatise on desirable attributes of security systems, see reference [1].)

In addition, the ways in which the need for security systems developed and solutions evolved have resulted in a plethora of different systems which are not only incompatible with each other, but also with other types of equipment used at the source, transit, storage or display chain. (Most obviously evidenced by the consumer environment situation, and the resultant quagmire of "opportunities" to be solved there.)

Today we find ourselves at the crossroads of a technological digital revolution; one where participation in going forward forces decisions to be made that involve significant departures from previous generation technology. This change begs the examination of opportunities to attain improvements over the current situation in several areas, such as consumer friendliness, compatibility and interoperability, improved security,...all topics where some degree of standardization has important potential. One of the more controversial areas is standardization of conditional access. The all-digital nature of compression systems provides at least the technical opportunity for future-friendly advances in this area.

STANDARDIZATION

The experiences of our industry with encryption products over the past decade has left a trail of both positive and negative reactions throughout the operator/user base. In addition the esoteric nature of cryptographic technology, in combination with the veil of secrecy that surrounds most products tends to shroud reality from view. The result is that decisions regarding the whole subject become driven in part by sound technical judgments and part by emotion.

The very mention of "standardized conditional access" in the wrong circles will frequently be met by cries of eventual disaster. Yet many who have studied the issue from a neutral position have concluded that when theory and experience are applied properly, there are indeed procedures and structures that can be implemented to provide some basis of commonality in future generation systems. Note the many non-military implementation standards used by the U.S. government and the longevity of the DES algorithm, for example.

The motivation for the consideration of standardization develops primarily from compatibility and interoperability issues. More and more relationship and interdependency exists today between heretofore unrelated markets. This trend will dramatically expand. The merging of the television and computer industries into a "multimedia environment" is in the sights of many wishing to put to use the broadband highways that lie in our future. The growth accomplished by these new markets will be throttled by interoperability issues.

Surrounding digital compression developments are significant efforts to define standards. Driven primarily through the International Standards Organization (ISO), the

global unification of digital television program generation, editing, storage, retrieval, transport and display is leading to a set of agreed upon methodologies for audio and video compression, and transport of complex multiplexes of associated data and ancillary digital services. These standards, known as "MPEG-2," cover the primary areas of audio compression, video compression and transport. They will serve as the guides to international utility of future systems for most industrial and consumer applications.

In the transport area, the work has led to the development of a working draft which defines:

- Program Stream—A grouping of audio, video and data elemental components having a common time relationship, and being generally "associated" for delivery, storage, playback, etc.

- Transport Stream—A collection of program streams or elementary streams (video, audio, data) which have been multiplexed in a non-specific relationship for purposes of transmission.

While discussions are continuing at the time of this writing, these "system layer" efforts are aimed at providing a basic data structure, the "semantics and syntax" of a data stream, that can serve as a common format for local and broadcast transmission.

Entities working within the ISO MPEG-2 System Layer Group have agreed to a number of basic structural elements that are expected to become part of the system layer syntax. Fundamental to this structure is that the transport stream will be "packetized"; that is, consist of packets of data (sizes of the packets are in the 130 byte to 192 byte range) containing digital information from a single elementary stream or data type. The packets will each be preceded by a "header" of up to 4 bytes of packet-specific information such as packet ID, clear/scrambled indicator, even/odd key, continuity counter and other information. The "generalized" digital nature of these packets makes for very flexible opportunities in the area of encryption and conditional access, and the packets can be easily and singularly protected (scrambled) throughout their distribution and routing "life."

In order for the digital television market to fully and freely develop, it is very important not only that specific audio and video compression techniques be codified, but this transport area as well. The requirements vary greatly between various applications for digital storage media (DSM) and direct broadcast satellite (DBS), for example. Yet it is essential that easy movement between such mediums be available. Many factors come into play, such as timing, program stream reconstruction, synchronization, de/remultiplexing, (re)packetizing, and of course the need for encryption in certain applications.

It has been an objective of the ISO systems working group to limit the extent of "specification" to a minimum...to define only as much as is generally agreed to provide meaningful interoperability. The remainder of this paper discusses the implications of encryption on interoperability, and the issues regarding separation of systems and long term security.

CONDITIONAL ACCESS RECOMMENDATIONS

Both the European (through the CCIR) and the North American (primarily through the ATSC) communities have considered the issues surrounding conditional access standardization, and both have extensive expertise and experience in the subject matter. The conclusions and recommendations of both groups are very similar [1],[2]; that:

> *conditional access systems can be designed according to fundamental theoretic principles and implementation procedures such that different systems can share certain common security elements without compromising security.*

It is helpful to observe the CCIR's definition of "conditional access," and note the two key elements which comprise it [3]:

- **Conditional Access System**—Within a television distribution system, the means to selectively provide television programs to specific individual subscribers. The system includes means to track access for accounting purposes.
- **Scrambling***—Alteration of the characteristics of a broadband video/sound/data service (i.e. television program or service) in order to prevent unauthorized reception of the information in a clear form. The alteration is a specific process under the control of the conditional access system (sending end).
- **Access Control**—The function of the conditional access control at the sending end is to generate the scrambling control signals, and the provision of information to enable authorized users to descramble the program or service. The availability of this information is controlled by the conditional access system, between the transmitter and receiver(s); thus information is structured in secure messages multiplexed with the signal itself.

So *conditional access* is the total envelope of mechanisms which are responsible for delivering information to selected receivers only.

In the context of system implementations and the above definitions, one notes that there is a natural segmentation between the requirements of a system's transport layer hardware-level *scrambling* elements and the addressing/authorization *access control* elements of almost any proto-typical system. In fact, the above distinct processes have become systemic to modern broadband system security approaches:

> The information (programming) to be transmitted is secured by scrambling (encrypting) the data during transit,
>
> The access control delivers to the decoder commands and procedures associated with who,

* The European Community has maintained the term "scrambling" as associated with the operations performed on the digital content of elemental streams and/or other raw services data. This is a holdover from the analog world where signal components were scrambled in the traditional sense. The U.S. community is adopting this terminology, which is convenient in separating the security mechanisms/algorithms used in the access control channel from those of the transport level data packet.

where, and when a decoder is allowed to unscramble the information and deliver the program.

In practice systems get very complex, and many factors must be considered. Assuming the scrambling process is done correctly from a cryptographic standpoint, it can be made very straightforward; essentially mechanical or generic. Access control is an area, however, where one finds much of the distinction between systems: how fast, how often, how user-friendly, how operator friendly,....It is in this domain that we find many of the processes that define a system's "personality" as well as those that control program access: PPV/IPPV procedures, cryptographic key distribution, all addressability processes, latency/synchronization factors, etc. Subscriber management systems, headend control systems, and system data channel(s) are dedicated to these functions, and *they are all unique to different system implementations.*

But what *can* be thought of as common are system services, especially if one considers that an MPEG-2 compressed version of a movie *can* be universally coded (the program stream), no matter what system is carrying it, or digital storage device is saving it. The scrambling of the signal is what has been recommended by the ATSC and CCIR as a factor that can be standardized on. The access control remains unique to each respective system, responsible for providing enabling parametric information (keys, etc.) to common descramblers.

SCRAMBLERS

The most straightforward method to secure a digital signal when presented in a bit serial fashion is simple modulo 2 EXOR of the data with a stream of random data. Of course the random stream cannot be literally random or the information will be thoroughly and permanently encrypted forever. For this reason, "pseudo random binary streams" (PRBS) are utilized...they look random to anyone not having certain "key" information.**

The basic premise that a *pseudo* random stream employed to scramble data can be essentially as secure as a truly random stream is a fundamental notion of modern cryptographic doctrine. When cryptographic systems are compromised it is not that this doctrine is at fault, it is that the design or the use of the PRBS generator is flawed, or (more often) that the other conditional access element, "access control," has broken down.

The basic argument that it is possible to standardize on the scrambler without compromising security is that all systems employ PRBS generators, or they can be modeled that way, and that no "good" PRBS generator is any better

** This approach is commonly used with a "private key" or symmetrical encryption approach which works well for high speed encryption and decryption. There are other techniques for encrypting information. The access control channels of most systems typically use other/additional techniques (e.g. public key cryptosystem attributes) to ensure that factors such as message authentication, message replay, and other kinds of spoofing, etc. are appropriately handled. These techniques are system-unique.

than any other "good" PRBS generator. That is to say if a given PRBS generator qualifies as good it must have certain qualities, and these qualities certify that it can be employed to generate pseudo random data that will be as random as any other generator of that quality.

Modern theory and experience, along with capabilities of today's digital electronics, allow the design of PRBS generators (and techniques for employing them to insure their inherent randomness is exploited) that meet nicely the requirements of today's systems. By accepting the qualification of "good" above, one has no argument that the scrambler/descrambler hardware cannot be standardized. This is a difficult notion to accept both intuitively and emotionally, and it may be a lost cause to expect it to be accepted. (Indeed, should the qualification process for defining "good" be flawed, the result could be disastrous, and that argument cannot be ignored.)

Ideally, to make everyone comfortable it would be nice to be able to change the scrambler if needed. The concept of changeable security leads to the next section.

ACCESS CONTROL AND REPLACEABLE SECURITY

Most newer system designs today employ (or will employ) some type of replaceable security hardware. This approach provides for the placement in a replaceable card or module some or all of the circuits associated with access control. Several systems in Europe have relied upon "smart card" technology for this capability.

Smart cards occur in four types [4]:

1. Small Memory Cards—Pay phone, gas station credit use,
2. CPU/Memory Cards—Banking, health care, pay TV, gaming use,
3. Large Memory/PCMCIA Cards—Sub-notebook, handheld computers,
4. "Super" Cards—Type 2 or 3 with on-card keyboard, displays.

The last type is not always technically a "smart card" in the sense that it might not follow the ISO 7816 or PCMCIA standards for physical size and I/O. It is included in this discussion for completeness, and to indicate where the state-of-the-art is progressing. In addition, there are other types of replaceable modules that have been developed and used for the computer, entertainment and security industries that provide functionality similar to smart cards.

But in the general sense of "changeable security" (which will become ubiquitous), with recognition that the access control portions of conditional access systems will most certainly remain unique among vendors, what all such approaches provide is an alternative to building into the decoder hardware permanent, and therefore potentially tamperable, security-related parameter storage and/or functional processing elements. The security card allows replacement of the access control functions of a system, or at least the cryptographically sensitive aspects of the access control, such that should it ever be necessary to update or change the system in this area, it is possible to do so.

The major trade-off surrounding system design employing

replaceable security cards is the decision about how much goes into the card? It turns out to be a question of economics. Security cards can cost from $2 to $30. The cost penalty for changing out a large system's population of security cards may well turn out to be less than the cost of tolerating piracy! But the degree of freedom allowed nevertheless has given the replaceable card a large popularity at this time, and the hard costs associated with more card functionality for fewer dollars continues to drop.

A natural breakdown between the access control and scrambler functions that constitute conditional access is to place the core "descrambler" circuits in the decoder hardware VLSI, and the system-specific (critical) access control functions in the replaceable card. One has to study carefully then the activity that takes place at the card interface to ensure that information available there, assuming total knowledge of what's in the decoder hardware, will not allow compromise of the system.

It would be better yet to place both descrambler and access control functions in the security card, but this can get cost prohibitive. The structure of the digital compression multiplex and packetization of elementary streams described above which may be concatenated and encrypted (scrambled) with different keys gives rise to a need for very sophisticated and high-speed logic in order to maintain operation at data rates to 50 or 60 Mbps! This kind of performance is not feasible in inexpensive replaceable cards, in combination with the demands that this would place on the card I/O and associated receptacle.

SUMMARY

The developing transport level definition of the MPEG-2 System Layer will result in a structure easily availing itself to a marriage of vendor-unique access control, and industry-wide common scrambling. Many implementation variations are possible, allowing the specific needs of each system designer/user to decide what form solutions are to take. Relative "levels" of security and risk assessments thereof can thus be weighed and appropriate requirements accommodated.

There are many advantages in having interoperable scrambling in the broadcast and storage arenas; this paper has not attempted to make those arguments. (References [1] and [2] are recommended reading for these discussions.) In the end, however, there will continue to be controversy, and commercial factors will dictate what the industry decides to do. But it is felt that there *are* compelling technical methods for how interoperability can be accomplished, and that these need to be (unemotionally) discussed.

REFERENCES

[1] Advanced Television Systems Committee Final Report T3/217. "Interoperability Among Alternate Media for the Delivery of Advanced Television Programming and Related Consumer Product Interface Issues," December 1992.

[2] CCIR Study Group II, Document 11/66. "Conditional Access Broadcasting Systems Recommendations," May 26, 1992.

[3] Stubbs, G.S., "Digital Compression, An Industry Process to Achieve Secure Conditional Access," *Communications Technology*, March 1992.

[4] Robinson, B. and M. Ryan, "Smart Cards," *Electronic Engineering Times*, March 29, 1993, p. 52.

About the Author:
Mr. Wechselberger has held various positions with TV/COM International (formerly OAK Communications) since 1980. His staff supports all of TV/COM's cable, satellite, and compression engineering initiatives and he is responsible for a number of key patents. Before joining TV/COM, Mr. Wechselberger was with the General Dynamics Electronics Division. He holds B.S. and M.S. degrees in Electrical Engineering and has published and lectured extensively in the fields of TV signal security, and general conditional access requirements involving communications, and encryption.