Secure Pay-Per-View Testbed

Dónal Cunningham
Donal O' Mahony
Networks and Telecommunications Research Group,
Department of Computer Science,
Trinity College Dublin,
Dublin 2, Ireland

Abstract

Trials of Video on Demand and Pay-Per-View systems are underway in many countries, and as a result, many cable and telecommunications companies are having to upgrade or replace their distribution networks. Video streams must be secure in order to prevent unauthorized viewing of the programs being transmitted, yet most existing security systems do not make use of the potential for bi-directional signalling in new and upgraded networks. It would prove more useful to many companies if they could use one system to test a number of different distribution networks to see if they gave an acceptable quality of service. In this manner, a company could decide if existing networks could be used without substantial changes, or whether expensive upgrades or indeed replacements were justified.

1 Introduction

In the past, cable television companies provided a basic service to their customers, consisting of the provision of a subset of the total number of channels, usually those freely available over the air or available at low cost. “Premium Channels,” usually film or sports channels, were supplied on a yearly basis to subscribers, who paid a flat fee irrespective of their viewing habits. The system did not permit customers to subscribe and unsubscribe to these channels prior to the showings of particular programs. “Pay-per-view” schemes permit exactly this — customers may watch programs on premium channels at any time, but only pay for the programs that they watch.

The main issue in PPV systems is that of administration. With most existing systems, customers are issued with some form of smart card on an annual basis, which permits access to the premium channels. Users can watch any program on any channel to which they are subscribed.

With systems used in the past, security was held to be assured because the smart card could not be reverse-engineered. Doubt has been cast on these claims[1]. These systems worked by passing encrypted video and/or audio data from the head-end station to the set-top boxes, which decrypted the data and displayed the results on the subscribers' screens. If bi-directional dialogues are possible, more secure systems can be used, which frequently exchange information securely between customer and head-end office.

Video Source

Most current approaches to premium viewing use analogue television channels. In recent times, it has become both practical and cost-effective to use digital video. This is typically produced in one of two ways, either

(a)using real-time encoding from a taped source ;
real-time encoders tend to be very expensive
or (b) captured and compressed off-line

When the later option is taken, the end product (a digital video stream) is typically stored on secondary storage (fast hard disks) or tertiary storage (optical or magnetic storage, typically CD-ROM or magnetic tape)[2]. In the future, film distributors may supply their customers with features in both analogue and digital form. Typically the most popular movies/programs will be kept on secondary storage and the less frequently-accessed items on tertiary storage. This is the approach taken by Digital, with their *Video and Interactive Information Architecture*[3].

Often the distribution network has a tree-and-branch architecture, and the most popular programs are cached at nodes in the tree serving <= 500 customers[4]. Since in a true Video on Demand (VOD) system there will be multiple concurrent accesses to the same file, caching reduces the complexity of the main video server as well as allowing a limited degree of fault tolerance.

The digital video coding scheme which predominates in the VOD and PPV markets is ISO Standard 11172[5] (MPEG). This uses block-based intraframe coding and bi-directional interframe motion prediction. Compression rates with raw digital video are typically up to 200:1. As a comparison, raw PAL video at "near-VHS" resolution (352 x 288, 25 frames/s) typically has a bandwidth of approximately 60 Mbits/s, whereas the same video data with associated audio can be encoded using MPEG with a bandwidth of 150 Kbits/s. MPEG decoding in software is currently only practical at low bit rates, and for VHS or near-VHS resolutions, must be done in hardware.

Distribution mechanisms

There are several possible distribution schemes[6]. These include

- CATV coaxial network using Analogue video streams
  One 6 Mhz analogue TV channel is used for each Interactive Video (IV) channel.
- CATV with Digital Modulation
  Several digital channels can be modulated onto one 6 Mhz digital channel, typically allowing data rates of between 3 and 30 Mb/s.
- Using a conventional telephone local loop connection
  Using HDSL[7] over short distances gives up to 1 Mbit/s, and using ADSL-I, -II or -III bit rates of 1.5 , 3 and 6 Mbit/s respectively can be provided over progressively shorter distances. Additional copper pairs can be employed to increase bandwidth.
- Fiber to the Kerb / Fiber to the Home
  These provides digital connectivity at speeds of greater than 155 Mb/s.
- ATM networks
  ATM's statistical time division multiplexing allocates bandwidth efficiently, and it usually runs on very high speed networks.

Upgrading existing coaxial networks is both challenging and expensive. Any cable company considering replacing parts of its network or any telecommunications company thinking of laying a new network needs to be sure that the network it is installing is capable of providing Interactive Video Services (IVS) for the near future and ideally has enough capacity for the medium-term future when it seems IVS will be extremely popular with subscribers. The bandwidth requirements for Video On Demand (where typically each subscriber tends to be assigned a unique channel) and Pay-per-View (where typically many subscribers share a channel) are quite different.

At the subscriber's location, a device called the *set-top box (STB)* sits logically between the distribution channel and the subscriber's television equipment. This box takes in the signal from the channel, decrypts it (assuming the subscriber has paid for the channel which he/she is trying to decode), decodes the compressed digital video and passes the corresponding analogue signal to the television. Some set-top boxes have extra functionality, allowing subscribers to plug in peripherals such as printers, joysticks, CD-ROMs, etc.

2 Existing trials

There are several trials underway both in the United States and Europe. With the FCC's 1991 “Video Dial Tone” ruling[8], telephone companies in the U.S., particularly the regional Bell operating companies, were permitted to transport and provide IVS in their regions under certain conditions. Many hardware & software manufacturers are forming alliances with network providers and are conducting trials of prototype IVS systems. Often these trials serve both as a feasibility test of the network and hardware and as a market trial to judge whether the potential subscriptions to the service warrant the heavy investment in R&D that will be needed.

VCTV Trial

This is predominantly a market trial being conducted jointly by AT&T Network Systems, US West and Tele-Communications Inc., under the name of Viewer-Controlled Cable Television[9]. The trial tests both Video on Demand and Pay-per-View services with 300 test users in a suburb of Denver, Colorado, and started in July of 1992. Half of the subscribers were offered VOD, and the other half PPV. The distribution channel is Fiber to the Home, and supplements the regular coaxial cable feed from the cable company. The source uses three UNIX processors to control a bank of S-VHS VCRs and controllers via a serial line, and uses an analogue scrambling technique. Digital RF channels are used to combine the multiple channels onto the fibre-optic trunk, and a bi-directional signalling path is provided.

NYNEX Trial

This trial[10] is currently underway in Manhattan, New York, and uses Digital's *Video and Interactive Information Architecture[3]* to test subscriber interest in VOD, home shopping and “other interactive programs.”

This trial follows on from Nynex's video-tone trial in Rhode Island, and is part of a test of the broadband network which Nynex is hoping to put in place in Northeastern U.S. “over the next decade.”

3 Security and PPV

The majority of existing systems for cable and satellite television transmission systems are analogue. Analogue encryption systems typically alter some of the fundamental characteristics of the video signal, e.g. the colour burst, horizontal sync, vertical sync[1]. They often invert and delay whole lines of picture information. Digital video encryption systems cut, rotate, invert and shuffle lines of the picture. With the advent of cheap, publicly-available electronic components hackers could easily and quickly build pirate decoders and descramblers, typically offering free updates to their customers within a few days of any changes made by the cable and television companies. As the analogue television signal cannot be *completely* scrambled (or else the decoder could not distinguish between noise and scrambled system), the pirate decoders latch on to the same signal transitions as the legal decoders. Digital systems typically alter lines in blocks, and do not use computationally intensive algorithms.

A real problem with existing security schemes is that the data transfer path is unidirectional. The cable company broadcasts to all of the set-top boxes (STBs), but can only estimate which STBs are receiving the data. The list of subscribers is a good indication, but a pirate smart card has the same supposedly unique ID as a legal card. The cable company can send out “bullets,” signals to switch off certain STBs, but the hacked cards/decoders have usually been tampered with so that this is ignored. Several methods exist to combat pirate STBs, but with the advent of bi-directional distribution channels and good-quality digital video, it makes sense to use traditional digital encryption methods such as asymmetric- and symmetric-key encryption.

Secure digital protocol

Symmetric-key encryption schemes such as DES are often less computationally-intensive than asymmetric-key schemes such as RSA. This leads to problems, as ideally we would like to encrypt all data with an asymmetric-key scheme, but do not have the computational power. It is possible that we may have it at the head-end, but the cost of developing a STB which could decode an asymmetrically-encrypted 30 Mbits/s digital video stream would be prohibitive. Using a symmetric-key scheme on its own is also infeasible, because the security of the whole system is based on one key. It is however possible to combine both asymmetric- and symmetric-key schemes into one system.

The *Video Stream* is encoded using a symmetric-key algorithm, and the key is changed at regular intervals. When a subscriber wishes to use a premium service, their STB engages in a dialogue with the head-end station over a low-speed asymmetrically-encoded channel, typically of the order of several Kbits/s. This channel is kept open, and is used to send cryptographic information relating to the Video Stream to the STBs. This is referred to as the *Control Stream.* The scheme also allows (if the cable company so wishes) one “seed key” to be sent to the STBs, which will then use another algorithm to produce subsequent keys to use in decoding the Video Stream. This method would free up the bandwidth currently used by the multiple Control Streams.

The head-end computer will keep a database of current connections, and can tell if two subscribers with the same ID are trying to obtain the same service. This will cause an alarm, and the data on the user whose ID was duplicated will be displayed. An option might be to allow duplicate connections so that a pirate user could be caught red-handed in countries where possession of a pirate decoder is legal, but the use of same is not. The database can also be used to assemble viewer statistics, enabling cable companies to target subscribers more accurately with a marketing campaign, for example.

In an ideal world, major cable operators could cooperate on a regular basis to see if STBs and/or subscribers were being used on more than one network. Confidential information need not be exchanged or security compromised, since the STB numbers give very little information (other than the number of decoders attached to a company's network) away.

4 Testbed Systems

There are many different video distribution systems in use today, and as outlined in section 1, there are equally many systems for cable and telecommunications companies to choose from. Operators would like to test prospective systems with a real-world application before committing themselves to installing a new network or upgrading an existing one. This is difficult, since many of the VOD and PPV systems being used in trials are incompatible. Hardware and software manufacturers have formed strategic alliances in the hope that their combined expertise will give them an advantage over their rivals. Cable & Telecommunications companies may not wish to commit themselves to a particular

hardware/software combination, and they are unable to compare different VOD/PPV systems as no existing application will run on multiple platforms.

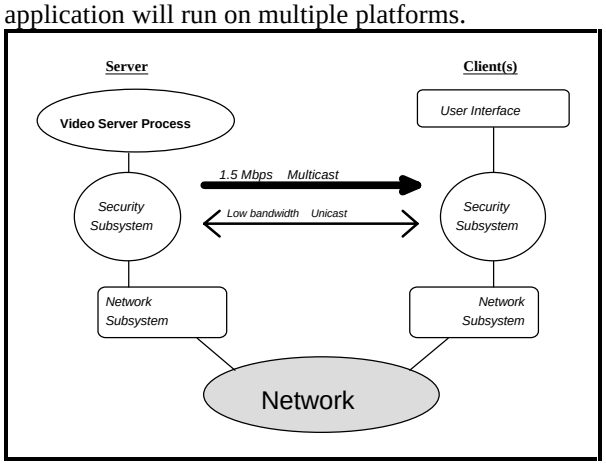

Figure 1 : TCD PPV System Architecture

The authors are currently constructing a network-independent PPV test system. The architecture is shown in Figure 1. MPEG video/audio streams are used, and the system is written in a modular fashion so that the interface between the Security and Network Subsystems is well-defined. As a result, only the Network Subsystem need be rewritten if the system as a whole is to be ported to a different network. The ability to work with an existing network may be useful where a company has already upgraded its network, and wishes only to test the network's ability to provide a PPV service. The Video Server is a high-performance PC Workstation with an AVI capture board. AVI files are converted off-line to MPEG, and sent over an Ethernet to a network of PCs and Sun Workstations with MPEG display capabilities. The Security Subsystem uses the twin stream approach outlined in Section 3, using a symmetric-key algorithm optimised for speed on the Video Stream, and an asymmetric-key scheme on the Control Stream. It is expected that the system will be complete in the Autumn of 1995.

Conclusion

The video distribution networks currently in use by cable and telecommunications companies in most cases need to be upgraded to provide Video on Demand and Pay-per-View services. Companies need to estimate the suitability of new networks for carrying VOD and PPV traffic, and also be able to compare these networks in a commercial light. Existing unidirectional broadcast security systems can be (and have been) broken, and networks with a bi-directional signalling capability should use security systems which take advantage of this capability to combat fraud and piracy. This paper has described a real-world system providing both robust security and portability to a wide range of networks, which would be very useful to cable and telecommunications considering implementing VOD or PPV systems.

References

[1] J. Mc Cormac, “European Scrambling Systems - Circuits, Tactics and Techniques”. Waterford University Press, Waterford, 1993.

[2] C. Federighi, L. Rowe. “A Distributed Hierarchical Storage Manager for a Video-on-Demand System.” *Storage and Retrieval for Image and Video Databases II,* IS&T/SPIE Symposium on Electronic Imaging Science and Technology, vol. 2185, pp. 185-197, 1994.

[3] Digital Storage Business Unit, “Video and Interactive Information Architecture". Digital Equipment Corporation, 1994.

[4] D. Deloddere et al. “Interactive Video on Demand,” *IEEE Communications,* vol. 32, no. 5, pp. 82-88, May 1994.

[5] D. Le Gall, “MPEG : A Video Compression Standard for Multimedia Applications”. *Communications of the ACM,* vol. 34, no. 4, pp. 305-313, April 1991.

[6] Y. Chang et al. “An Open Systems Approach to Video on Demand.” *IEEE Communications,* vol. 32, no. 5, pp. 68-80, May 1994.

[7] T. Hsing et al. “Video Communications and Services in the Copper Loop.” *IEEE Communications,* vol. 31, no.1, pp. 62-68, January 1993.

[8] FCC Docket No. 91-334, *Video Dialtone Order.* November 22, 1991.

[9] J. Allen et al.“VCTV: A Video-On-Demand Market Test.” *AT&T Technical Journal,* vol. 72, no. 8, pp. 7-14, January/February 1993.

[10] G. Bates, *Press release CORP/94/465.* Digital Equipment Corporation, May 1994.