DOWNLOADABLE SECURITY

James William Fahrny
Comcast Cable Communications

Abstract

This paper will define a common security architecture that overcomes some of these obstacles and issues described in the background section above. This common hardware security platform can be used to secure Broadcast Conditional Access systems, Video On Demand services, Digital Rights Management, and the Authorized Service Domain services in extending CA into the home network.

This proposed paper would cover the following topics:

- *Architecture Block Diagram of the Downloadable Security System*
- *Description of the secure download mechanism and how it can be secured.*
- *Analysis of how this advances security for video and audio content*
- *Definition on how this can be used to perform "Hardware Renewability" with a software download using FPGA technology.*
- *Describes how the paradigm of revocation and renewabilty are modified for a better customer experience.*

Analysis of how the downloadable features can be applied to various applications of the hardware platform including CAS, VOD, DRM, Trusted Domain, Streaming and Personal Computing

BACKGROUND

Conventional implementations of media (e.g., video, audio, video plus audio, and the like) program stream delivery systems (e.g., cable, satellite, etc.) include a head-end where the media programming originates (i.e., is encoded and compressed, groomed, statmuxed, and otherwise appropriately processed), a network (e.g., cable or satellite) for delivery of the media programming to the client (i.e., customer, user, buyer, etc.) location, at least one set top box (STB) at the client location for conversion (e.g., decryption and decompression) of the media programming stream, and at least one respective viewing device such as a television (TV) or monitor that is connected to the STB. Alternatively, the STB may be eliminated, and decryption and decompression may be implemented in the receiving device.

Conventional head-ends and STBs employ particular matching encryption/decryption and compression/decompression technologies. However, there is little standardization of particular matching encryption/decryption across media program stream delivery system vendors. The encryption/decryption and compression/decompression technologies in the particular conventional system are fixed and often proprietary to the vendor. Furthermore, conventional media service processing and delivery systems typically implement security processes in connection with individual implementations of point of deployment, CableCard, Smartcard, etc. systems.

Transitions to upgrades in encryption/decryption and compression/decompression technologies are, therefore, expensive and difficult for the media program stream delivery system vendors to implement. As such, customers can be left with substandard service due to the lack of standardization and the reduced competition that the lack of standardization has on innovation in media service delivery. The lack of standardization also restricts the ability of media service providers to compete. For example, customers may have viewing devices that could take advantage of the improved technologies; however, media stream delivery system upgrades may be impossible, impracticable, or not economically feasible for vendors using conventional approaches. A significant level of customer dissatisfaction or vendor cost may result and the ability of media service providers to improve service and/or add new services is greatly restricted.

Thus, it would be desirable to have a system and a method for CA download and reconfiguration that overcomes the deficiencies of conventional approaches.

SUMMARY

This paper generally describes an improved system and method for security processing digital media streams. The improved system and method for security processing media streams of the present invention may be compatible with previously used (i.e., legacy) systems and methods using all levels of media stream processing and delivery service (i.e., basic to high-end) as well as adaptable to future implementations, and that is flexible, renewable, re-configurable, and could support simultaneous multiple security systems and processes.

This paper proposes a method of multi-stream security processing and distributing digital media streams. The technology comprises generating encrypted digital media streams. The method further comprises coupling a network to the head-end and receiving the encrypted digital media streams at the network. The technology yet further comprises coupling at least one receiver to the network and receiving the encrypted digital media streams at the receiver, and presenting a decrypted version of the encrypted digital media streams using the receiver. At least one of the head-end and the at least one receiver comprises a security processor that may be configured to provide at least one of simultaneous multiple encryption and simultaneous multiple decryption processing of the digital media streams.

This paper describes a system for multi-stream security processing, key management, and distributing digital media streams, a security processor configured to provide at least one of simultaneous multiple media transport stream decryption and encryption processing is provided. The single chip solution described in this paper includes a security processor, a controller and a plurality of digital decryption engines. The digital decryption engines may be selectively parallel coupled by the controller for simultaneous operation in response to a predetermined security configuration.

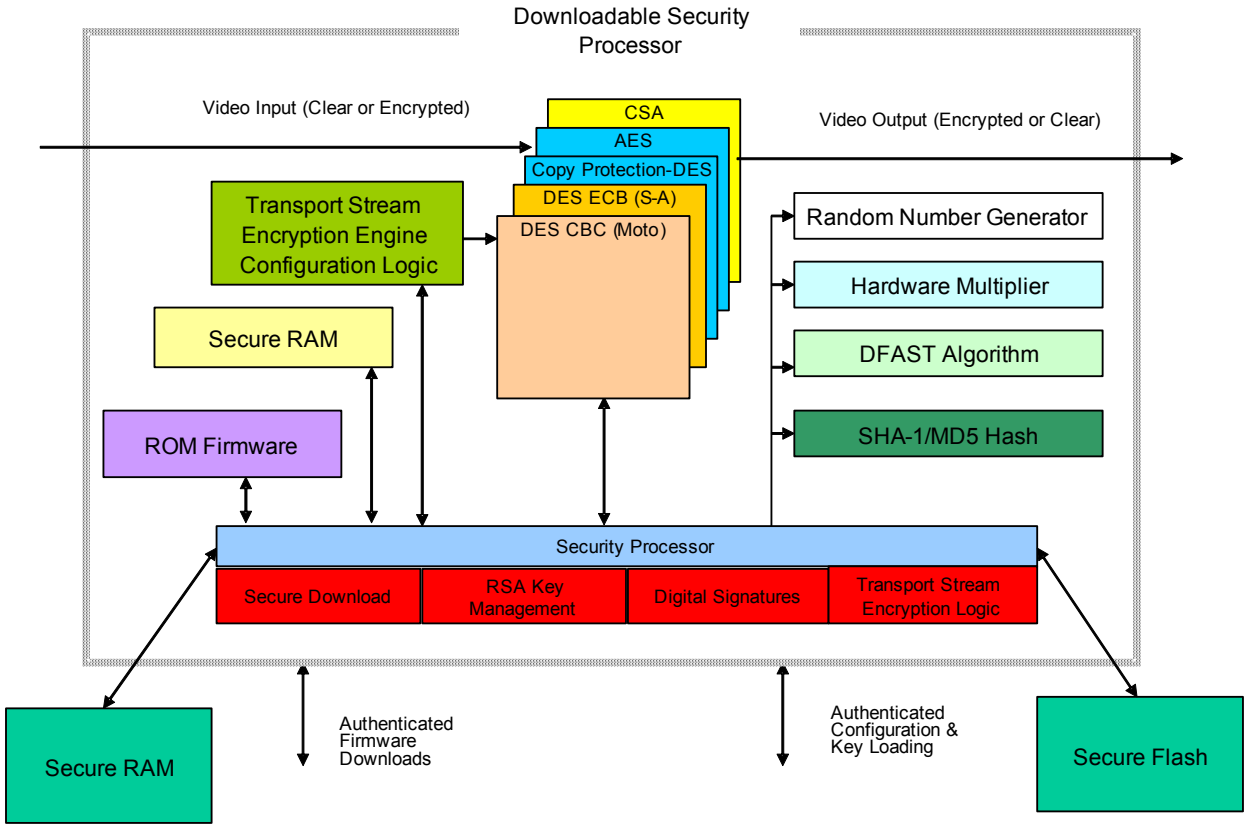
Though this paper describes a future vision Security System On a Chip (SSOC), the current technology widely deployed is done with separate physical devices. The Large Scale Integration (back-end) device contains all codecs, transport functions, de-compression, general purpose processor, memory, and other subsystems. The

Security Processor is a separate chip since it typically has on-board flash memory and numerous layers of tamper resistance and countermeasures to prevent hacker attacks. Based on current device fabrication technologies, the SSOC is not the most cost effective solution though it can be made more secure. In the future, there may be technology that enables the SSOC in a cost effective manner by including or replacing all of the tamper systems and countermeasures on the larger device.

ARCHITECTURE

The following diagram defines the elements of a downloadable and re-configurable security processing system. This diagram includes the key management system and secure down load system to install a new key management system. In addition, the re-configurable security transport system is defined as part of the overall technology.

The following diagram shows a single block diagram, which is a logical representation. The transport stream decryptors can be packaged in a separate integrated circuit (IC) with the other set-tops functions like decoders, demux, graphics engines, etc. When the system is packaged separately, there must be methods implemented to secure communications between the transport stream decryptors and the security processor in the client device. This security is not in the scope of this paper.



Authentication

When devices are installed on a cable network for the first time, a discovery process must occur. The Head-end server would broadcast an announcement message much like a DHCP server. The client will respond to the "announce" message with credentials to authenticate the client security processor. The head-end server will then present its credentials to the client security processor so that the client device can trust the server and the server can trust the client security processor. Credentials are presented with digital signatures for authenticity and the public key is used to verify the credentials on the receiving device.

Download: Obtaining a client's network personality

Once the server trusts the client security processor and the client security processor trusts the server, the security processor determines whether it needs a personality in the form of a security client depending on the network information that it receives in the authentication process. If a download is required, a secure key exchange occurs to setup for the transfer of an encrypted and digitally signed security image to the security processor in the client device. Once the client is validated through signature verification and decryption, it is loaded into the security processor and executed.

This process permits a security processor to obtain its security personality (Scientific-Atlanta, Motorola, NDS, Nagra, etc) when it checks into securely the first time. This technology also allows a device to move from one network to another whereby the client will determine that it has incorrect security client software loaded, and deletes it from memory. At this time, the client security processor will request the head-end server to download a security client for the new network personality. Finally, the secure download process can be used to simply upgrade the key management methods while preserving entitlements, purchases, credits and other important data stored in the security processor.

SECURING THE DOWNLOAD

The anchor of security and trust within this technology is in the security of the download. The client should ONLY be able to download new firmware when the head-end server commands the client to receive a new download. The client should not be able to force a download outside of the proper network personality changes. If any of this is incorrectly design, the overall security is subject to severe compromise. To accomplish this strong security, the head-end must "unlock" the download ability of the client security processor. If the client is locked, the security processor cannot be loaded with a new client.

In the same way, the image being sent to the client security processor must not be tampered and likely has elements of data that should not be viewed. This leads to the use of digital signatures and symmetric encryption of the image. The signature protects the image from being modified and the encryption protects data elements from being viewed.

ADVANCING CONTENT SECURITY

In the current systems, there are typically no methods to upgrade the system for fear that tampering or countermeasures would be more easily installed. Therefore, most components in the security architectures are constructed so that they cannot be modified.

This can be great from a security view but leaves no ability to adapt to the changing world of content and content delivery systems.

The system proposed in this paper is not as static with the secure download mechanism and therefore creates new abilities in support of potential business models as they are developed. Similarly, the longevity of a renewable security system that can adapt over time but remain secure appears to be greater than conventional security methods.

USING SECURE DOWNLOAD FOR HARDWARE RENEWABILITY

There is another unique development that recently presented itself in the development of this technology. Field Programmable Gate Arrays (FPGA) have been used LSI hardware components where one can develop hardware logic and load the logic language into an FPGA to achieve dynamic hardware. This technology has been very expensive in the past.

However, recently IBM and other research facilities have developed FPGA technology in 90 nanometer geometries of chips that is extremely cost effective. One could effectively include 4,000 to 10,000 gates of FPGA into a security processor and leave it blank for future use. If a new algorithm is required because something is compromised, the FPGA could be used to create a hardware accelerator of a new algorithm. In this case, all of the client security processors would be downloaded with hardware logic that would be loaded into the FPGA section of the security processor to enable the new algorithm.

CHANGING THE PARADIGM: RENEWABILITY INSTEAD OF REVOCATION

One of the largest problems in security systems is that of revocation. Revocation is very operationally unfriendly to manage and is really built in a manner to not have a large scale system revocation of keys. The single biggest issue with revocation is that a revocation event typically disables legitimate customers experience.

In this Downloadable Security system, we propose that the renewability be used in place of revocation in all cases possible. Since this system can securely transport data from the head-end server to the client security processor, keys of many types (authentication and encryption) can be renewed when compromised or periodically if desired. Clearly, if keys are renewed in a “live” system, synchronization of the transition must be managed using a solid time base so that the customer experience is completely uninterrupted.

In any case, this system provides a much better possibility with renewal since the compromised systems are not actively shutdown but is passively allowed to expire when the crypto period of their entitlements end. Paying customers are then renewed in this process to a new key set so that their experience is uninterrupted.

FUTURE APPLICATIONS

This technology was developed to focus on a certain set of problems in the Broadcast Conditional Access domain. However, after further review, this technology will be very effective if applied to On Demand security, Home Network Content distribution, Trusted Computing Platforms, Digital Rights Management, and Interactive Gaming.

In fact, this technology is so flexible that one could deploy a product with the security processor hardware and a specific security application or profile. Later the security processor could be upgraded to add security management for one of the other technologies as it is added as a service to the network.

For example, a system could be deployed with broad CAS and later be upgrade to support VOD, or Home Network Content security with a secure upgrade in the field.

CONCLUSIONS

To summarize, we believe that the Secure Download technology described in this paper will provide the next generation of security for Broadcast, Video On Demand, and Streaming media systems. If the Large Scale Integrated (LSI) devices are design with some flexibility for the future, this system will have a tremendous longevity and a strong ability to counter any hacker attacks to steal services or clone devices in the field for signal theft.

In the same way, we believe that the usage of this technology will grow with time since we are only viewing the initial stage of this new paradigm at the present time. Applying this technology to Home Networking, IP video delivery systems or even Digital Rights Management will increase greatly over the next couple of years.