Integrating Network Security Mechanisms into a DVB-T Network

C. MANIFAVAS
Technological Educational Institute of Crete
Security Systems Laboratory
Estavromenos, 71500 Heraklion
GREECE

A. SIDERIS
Technological Educational Institute of Crete
Telecommunications Systems Laboratory
Estavromenos, 71500 Heraklion
GREECE

P. FRAGOPOULOU
Technological Educational Institute of Crete
Network Systems Laboratory
Estavromenos, 71500 Heraklion
GREECE

V. ZACHAROPOULOS
Technological Educational Institute of Crete
Telecommunications Systems Laboratory
Estavromenos, 71500 Heraklion
GREECE

Abstract: The provision of broadband interactive services is one of the capabilities offered by the Terrestrial Digital Video Broadcasting (DVB-T) standard with the use of various return path technologies (i.e. WLAN, DSL, etc.). Because of its broadcasting nature, protection of the sensitive user data (credit car numbers, passwords e.t.c.) encapsulated in the DVB-T MPEG transport stream is needed since any adversary can receive the data intended for a legitimate user by just using a laptop and a DVB-T receiver card with its appropriate software. In this way, the adversary can extract the unprotected IP traffic from the received MPEG-TS stream. Furthermore provision must be taken to secure the return path channels and access networks which are used for the communication of the endusers with the DVB-T platform. We tackled the problem from three different angles. Firstly, security at the back haul network (the DVB-T UHF downlink and the corresponding return path/uplink) using IPsec. Secondly, security at the access network (WLAN network that provide to end users access to the services under consideration) using IEEE802.11i & FreeRadius. Thirdly, end-to-end security (client-server interactions where the server resides in the DVB-T service provision domain) using SSL. This paper presents a number of mechanisms which are used to secure interactive IP traffic (i.e. audio/video on demand, client-server services, etc.) conveyed over a prototype DVB-T implementation.

Key–Words: Terrestrial Digital Video Broadcasting, Interactive IP Services, Security, Privacy

1 Introduction

The European Union (EU) issued a directive in 2005 recommending Member-States to switch to digital terrestrial television transmission by 2012 [1]. This switch includes the use of DVB-T (Digital Video Broadcasting for Terrestrial) [2] as the broadcasting standard. DVB-T's ability for combining in a single transport stream digital TV programmes and IP data, while being able to transmit this stream in UHF over a large geographical area and at a high data bit rate, led to the deployment of DVB-T networking infrastructures which are used not only for the provision of digital TV programmes but also for the provision of interactive services (IP TV/Radio, Internet, e-mail) to the end-users. In such deployments and in order to provide to the end-user interactivity, return channels (WLAN, PSTN) are used to carry the requests to the providers while the services are provided through the UHF link.

Because of the broadcasting nature of DVB-T, the end-users sensitive data (credit car numbers, passwords e.t.c.) which are encapsulated in the DVB-T MPEG transport stream can be received by any third person (adversary) by using a laptop and a DVB-T receiver card with its appropriate software. In this way, the adversary can extract the unprotected IP traffic from the received MPEG-TS stream. The failure of protecting end-users/customers from these events can not only incur financial loss but also undermine customer confidence in using the platform for the purpose indented. It is obvious that the integration of security mechanisms in the DVB-T networking infrastructure is a necessary action that not only will prevent any adversary to exploit sensitive data but it will enforce the trust of the customers to the DVB-T system.

In this context this paper examines a DVB-T networking infrastructure -located in Heraklion of Crete- which is used for the provision of interactive services to the citizens of the city and identifies its weak points in terms of security. Finally it implements the necessary security mechanisms which will provide the following services:

- **Authentication:** assurance that the communicating entities are those claimed
- **Confidentiality:** prevention of the disclosure of information to unauthorized parties
- **Integrity:** prevention of unauthorized modification of information
- **Non-Repudiation:** protection against denial by one of the parties in a communication
- **Access Control:** prevention of unauthorized use of a resource

Following this introductory section the rest of this paper is organized as follows: Section 2 presents the DVB-T architecture, Section 3 describes the testbed, analyses the security needs and gives the implementation of the proposed security mechanisms, while Section 4 concludes.

2 DVB-T system overall architecture

The architecture of the examined DVB-T system which is already constructed under an EU funded project [3, 4] is depicted at figure 1. The overall architecture comprises two subsystems: a) a number of cell main nodes (CMN), and b) a central broadcasting point (DVB-T platform).

Each CMN enables a number of end-users/service-providers (geographically neighbouring the CMN) to access/provide IP services respectively through the DVB-T network. The communication between the end-users/service-providers and the corresponding CMN is achieved via broadband point-to-multipoint links (i.e. WLAN, xDSL) and it constitutes the access network. All the IP traffic stemming from its senders is gathered by the CMN and is forwarded to the central broadcasting point via dedicated point-to-point links (return path channels-uplinks) such as PSTN/ISDN, WLAN, xDSL, UMTS, GSM.

The broadcasting point receives all the IP traffic stemming from all the CMNs, where an IP encapsulator unit filters, regenerates and multiplexes all the IP traffic in a single DVB-T stream along with digital TV programmes stemming from the TV broadcasters. The DVB-T stream is then broadcasted in UHF. Every user receives the requested IP services through its corresponding CMN. Both the UHF downlink path and the uplinks comprise the backhaul network.

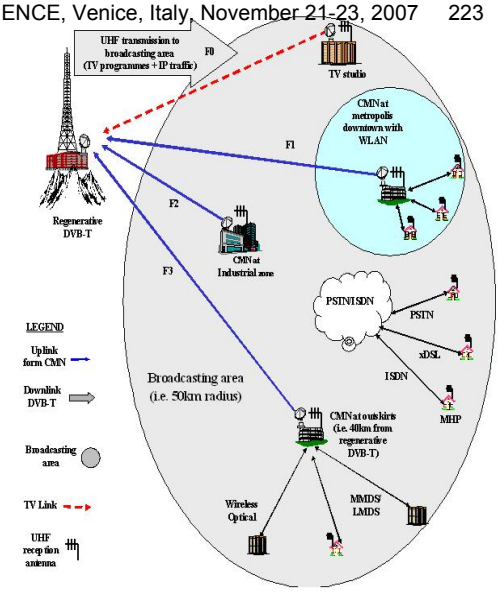

Figure 1: DVB-T architecture.

In such a configuration both reverse and forward IP data traffic are encapsulated into the common DVB-T stream, thus improving the flexibility of the network by offering interactive services. The above configuration has been set-up and running in Heraklion city since August 2004, serving as the ATHENA FP6-507312 IST project demonstrator.

3 Testbed & Security Implementation

The testbed used for the work carried out in this paper is depicted on figure 2. The users could send their requests to the VoD (Video on Demand) server through the access network (802.11g) and the uplink (dial up) while the replies were sent back through UHF where upon receipt from the CMN the replies were forwarded to the respective user. Taking into ac-

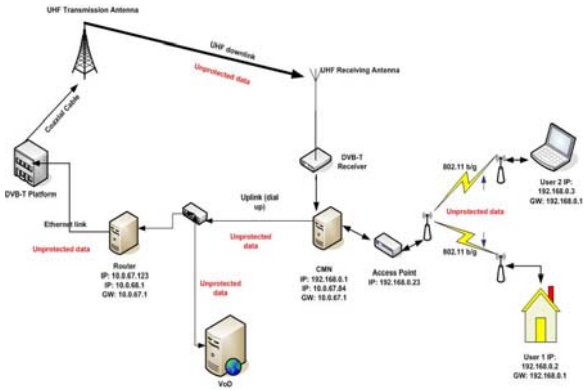

Figure 2: Implemented Testbed.

count the above implementation which conforms to the architecture presented on figure 1 the following speculations can be made for the need of security provision on the system:

- Security provision on the access network.
- Security provision on the backhaul network.
- Security provision on the application level (end to end security)

More specifically on the access network and especially because a WLAN (802.11b/g) technology is used, the need for end-users authentication/authorization and data encryption is obvious since in the opposite case anyone could connect to the system and use its resources for its own purpose and /or steal sensitive data from the legitimate end-users.

On the backhaul network the need for protection of the data travelling the uplink and the downlink is mandatory. Especially at the downlink and because of the broadcasting nature of the DVB-T any non legitimate user could receive the broadcasted stream with the use of a laptop and a proper receiver card (DVB-T aware).

The use of security mechanisms on the application level provides real and to end security since the transferred data are protected before even leaving their source (assuming that the source is not already compromised). This kind of protection could eliminate the need for security mechanisms at the backhaul and the access network (except the need maybe for authentication and authorization) thus preventing the DVB-T network from additional overheads and CPU processing. Unfortunately not all applications support effectively security mechanisms therefore the protection of their data by securing their travel paths (links) remains as a need.

3.1 Security at the Access Network

At the access network, the security standard IEEE802.11i, ratified in June 2004, and an open source implementation (FreeRadius [5]) of Remote Authentication Dial-In User Service (Radius) protocol [6] have been used to provide authentication, confidentiality, data integrity and authorization to the end users of the DVB-T platform.

The above security requirements were met by using the following:

- IEEE802.11i standard :
  - Counter Mode with CBC-MAC Protocol (CCMP) [7] which is a new protocol, designed from ground up. It uses Advance Encryption Standard (AES) as its cryptographic algorithm. CCMP provides data integrity and confidentiality.
  - IEEE802.1X Port-Based Network Access Control: IEEE802.1X was used with Protected Extensible Authentication Protocol (PEAP/MS-CHAPv2) as authentication method [8].
- FreeRadius as back-end authentication server and authorization Server.

The use of CCMP in conjunction with IEEE802.1X is also known as a Robust Security Network (RSN) or WPA2. Figure 3 shows the implemented security scheme on the access network. The end user is called Supplicant, the Access point (AP) is called Authenticator and the FreeRadius is called Authentication Server (AS). The following

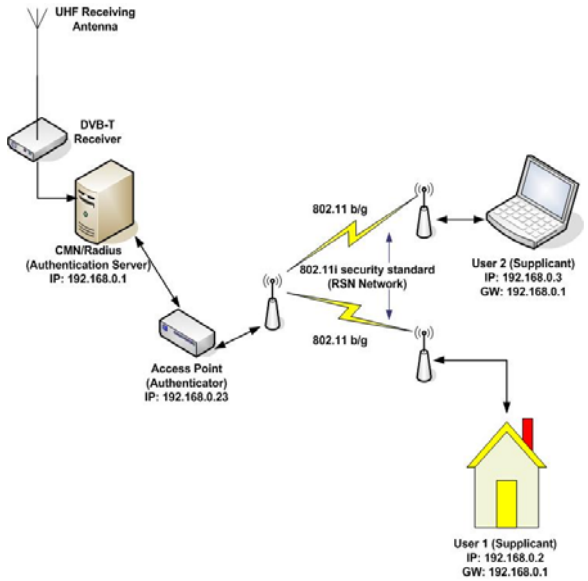

Figure 3: Security on the access network.

steps take place when an end user requests access to the network (authentication/authorization process):

- The AP asks for the Supplicant's identity (username/password). No other traffic than Extensible Authentication Protocol (EAP [9]) is allowed before the Supplicant is authenticated.
- A TLS tunnel between the Supplicant and the AP is being set up.
- The Supplicant sends its identity to the AP.
- The AP encapsulates the received EAP messages in RADIUS format and sends them to the AS.
- During all the authentication operation the AP relays the packets between the Supplicant and the AS.
- If the authentication is successful the AP grant access (opens the port) to the Supplicant and other traffic than EAP (like IP) can be send/received otherwise the port remains closed for the Supplicant.

After a successful authentication all the traffic between the supplicant and the AP is encrypted with AES. The keys needed for the encryption are derived from 802.11i standard extended key derivation/management mechanism. The operations described above provide a robust security solution to the access network.

3.2 Security at the Backhaul Network

At the back haul network the IPsec mechanism is used to provide authentication, confidentiality, data integrity and denial of service protection to the end users of the DVB-T platform. IPsec is a framework for security that operates at the network layer by extending the IP packet header and provides security to the IP and the upper-layer protocols [10, 11, 12, 13].

Figure 4 shows the implemented security scheme on the back haul network. All IP traffic sent and received from the end users passes by the uplink and downlink of the back haul network. The main concern is to secure all the IP traffic transferred from the DVB-T platform towards the CMN (UHF downlink) and all the IP traffic transferred from the CMN towards the DVB-T platform (uplink). The IPsec end points for the downlink/uplink can be seen at Figure 4 (IPSec End-point A and B). The ESP protocol was chosen since it provides authentication and encryption. The tunnel mode was the obvious choice in order to provide a virtual "secure hop" for all the IP traffic between the end points.

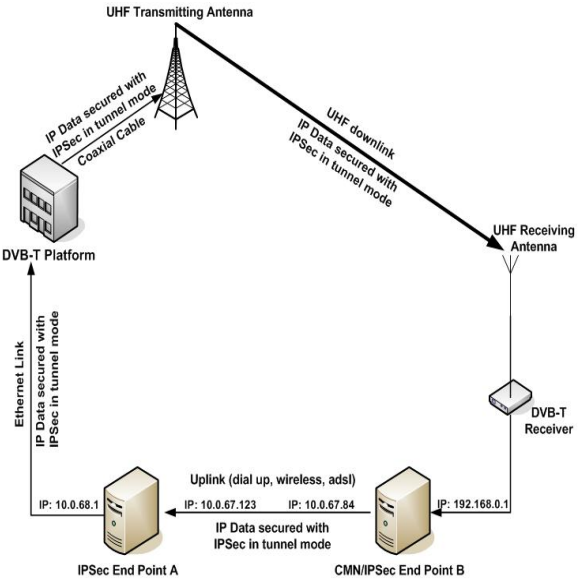

Figure 4: Security on the backhaul network.

3.3 Security at the Application Level

One way to implement end-to-end security is by using the SSL protocol [14]. End users (clients) interact with servers residing in the DVB-T service provision domain. In our case (see figure 5), an SSL enabled server sits within the DVB-T platforms broadcast point. This server can offer a number of services (e.g. audio/video/data on demand). We implemented

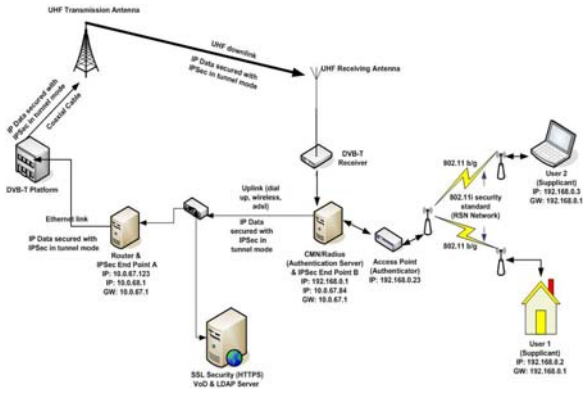

Figure 5: SSL security.

a Certificate Authority (CA) that signs and publishes X.509 identity certificates. The client is configured to trust the CAs certificate that signed our data server certificate. The following steps take place when an end user requests access to a network service:

- A user accesses an SSL enabled web server and verifies its certificate.
- The server requests and verifies the client certificate.
- The server checks for a valid client UID and password stored in an LDAP.
- The server checks whether the client is allowed to use the requested service via group memberships stored in LDAP.
- After successful authentication and authorisation the users is granted access to the service requested.

4 Conclusion

The DVB-T standard provides the ability to combine digital television and IP data in one UHF beam and broadcast that beam to users that are dispersed over a wide area. Because of its broadcasting nature, protection of the sensitive data transmitted encapsulated in the DVB-T MPEG transport stream is needed. Without this protection any adversary can receive the data intended for a user by just using a laptop and a DVB-T receiver card with its appropriate software. Furthermore extra precaution must be taken when DVB-T is used to provide IP interactive services since in

this case return path channels of various technologies are used. In such configurations the backhaul network (DVB-T downlink and CMN uplinks) and the access networks are also susceptible to threats from non legitimate entities.

Taking into account the above, the IPsec security mechanism was used to provide a robust security solution to all the transferred data from and towards the DVB-T platform (backhaul network). Furthermore, additional measures had to be taken in order to prohibit unauthorized access to the provided network services. The security standard IEEE802.11i and FreeRadius have been used to provide authentication, confidentiality, data integrity and authorization to the end users of the DVB-T platform. For services provided from servers reside in the DVB-T SSL enabled solutions were used to provide a reliable end-to-end service.

In the future we plan to integrate other security technologies within the prototype DVB-T implementation used as testbed. These technologies include OpenVPN (operates at the transport layer in contrast with IPsec that operates at network layer), smartcards that will store and process cryptographic keys and digital certificates used to authenticate the CMN and decrypt the received UHF beam. Furthermore we plan to develop a mechanism that will detect when an application can or uses already a security mechanism (e.g. SSL) so in that case the corresponding traffic (application data) will not have to pass from the IPSec processes. This will result to less networking and processing overhead over the DVB-T system. To reassure that the implemented security schemes do not cause a serious performance degradation and therefore impact the QoS of the provided IP services, an evaluation and comparison of the different techniques used will be performed.

Acknowledgements: The work presented in this paper is co-funded by the European Social Fund and National Resources (project EPEAEK - ARXIMIDIS - Kerveros).

References:

[1] Commission of the European Communities, *"Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, on accelerating the transition from analogue to digital broadcasting"*, COM(2005) 204 final, Brussels, 24.05.2005.

[2] ETS 300 744: Digital Video Broadcasting (DVB): *Framing structure, channel coding and modulation for Digital Terrestrial Television (DVB-T)*, ETSI, 1997.

[3] Digital Switchover: *Developing Infrastructures for Broadband Access, Information Society Technologies, FP6-507312, 6th Framework Programme, Specific Objective "Broadband for All"*

[4] E. Pallis, C. Mantakas, G. Mastorakis, A. Kourtis, V. Zacharopoulos, *"Digital Switchover in UHF: the ATHENA concept for broadband access"*, European Transactions on Telecommunications, Vol. 17, Issue 2, 29 March 2006, pp. 175–182

[5] FreeRADIUS Server Project, http://www.freeradius.org.

[6] RFC2865: *Remote Authentication Dial In User Service*, http://www.ietf.org/rfc/rfc2865.txt.

[7] RFC3610: *Counter with CBC-MAC (CCM)*, http://www.ietf.org/rfc/rfc3610.txt.

[8] RFC3580: *IEEE 802.1X RADIUS Usage Guidelines*,http://www.ietf.org/rfc/rfc3580.txt.

[9] RFC3748: *Extensible Authentication Protocol (EAP)*, http://www.ietf.org/rfc/rfc3748.txt.

[10] RFC4301: *Security Architecture for the Internet Protocol*, http://tools.ietf.org/html/4301.

[11] RFC4302: *IP Authentication Header*, http://tools.ietf.org/html/4302.

[12] RFC4306: *Internet Key Exchange (IKE)*, http://tools.ietf.org/html/4306.

[13] RFC4309: *Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)*, http://tools.ietf.org/html/4309.

[14] RFC2246: *The TLS protocol (v. 1.0)*, http://www.ietf.org/rfc/rfc2246.txt.