Secure Video-on-Demand Server Project: Requirements and Solutions.

JOSEP PEGUEROLES VALLÉS AND FRANCISCO RICO-NOVELLA

Telematics Engineering Department.
Polytechnic University of Catalonia.
MODC3 D320 c/ Jordi Girona 1-3 08034 Barcelona
SPAIN.

Abstract:- When cryptographic techniques are added to advanced network services such as Multimedia-on-demand many aspects have to be considered. Especially, when commercial services are being offered, aspects related to secure payments, server fraud protection and client rights have to be studied. The Security Module in SSADE (Secure System for the Access and Efficient Distribution of Multimedia-on-Demand Services - CICYT TEL99-0822) has centered his investigations in two main items: Secure and Anonymous Payment and Ciphering Techniques for protecting data from eavesdroppers. This paper will focus in the solutions adopted in this project in order to achieve secure access and payment to the Multimedia-on-Demand service and privacy for content distribution.

Keywords:- video-server security, access, secure payment, secrecy.

1. Introduction

Troubles related to bandwidth and QoS are being gradually overcome in current multimedia communications and security concerns are getting increasing significance in data, voice and video transmissions. When cryptographic techniques are added to advanced video services such as video-on-demand many aspects have to be considered.

First of all multimedia requirements are very time-restrictive. This is why unreliable protocols such as UDP are used, so ciphering techniques cannot rely on transport protocol and they may be fitted to isolated protocol data units (PDU), in any other case, a packet loss will cause forward errors.

Secondly, ciphering algorithms should not increase significantly the packet delay. If this occurs, security increase will lead to visual quality decrease or excessive transmission delay, and interactive services will not be possible.

Finally, when commercial services are being offered, aspects related to secure payments, server fraud protection and client rights have also to be studied.

The Security Module in SSADE (Secure System for the Access and Efficient Distribution of Multimedia on Demand Services) has centered his investigations in two main items: Secure and Anonymous Payment and Ciphering Techniques for protecting data from eavesdroppers.

The rest of this paper is organized as follows. Section 2 presents our Server Architecture and divides service timing in two phases: reliable transport and unreliable transport phase. Next, security services required are analyzed. Section 3 deals with services concerning the reliable transport phase, that is, secure access and anonymous payment. Section 4 describes how our system achieves secrecy over unreliable protocols. Finally, Section 5 presents conclusion and future work.

2. Video Server Architecture.

Typically, a multimedia server works as sketched in Figure 1.

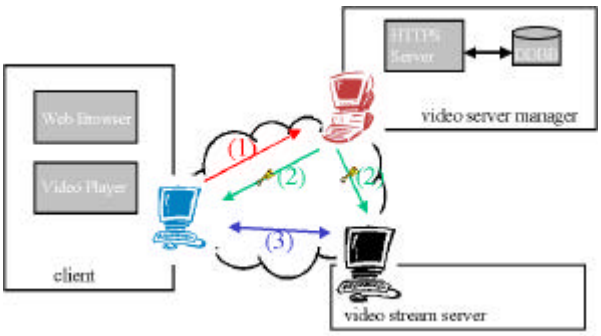

Figure 1. Communication steps in video server architecture

When a client wants to view any multimedia content, it accesses the server Menu via a web browser (1). After that, the client can select his own preferences (film or content to retrieve, speed connection, quality requirements, etc.). Once the server knows exactly what the client wants, it asks for a payment. When this is done, the server returns to the client the data he will need in order to get the multimedia stream (2). Usually, it gives to the client the name of the host where the data can be found and a socket where to connect. It also sends the data and keys needed to the server host (2). Then it will be able to authenticate the client and cipher the video stream. Finally, the client is able to connect to the video stream server to get the purchased content (3). [1]

2.1. Security Threats and Services

When using open networks, security troubles become important. In the mentioned model a very weak point is showed up: communication via Internet [2].

First, the Security Module must protect the information that the client sends to the server to order the content. Second, it must warrant that the payment will be done properly and that no participant in the transaction will be harmed. Finally, multimedia data have to be protected from malicious third parties or eavesdroppers.

According to the former paragraph, the services to study are: secure access via web over reliable protocols, secure payments via web and data secrecy over unreliable protocols.

Since these three steps are done over different transport protocols we will divide the security services in our system into two phases: secure services over reliable protocols: that is, authentication and payment; and secure services over unreliable transport protocols, that is to say, secrecy.

Next sections deal with the solutions adopted in our project in order to implement these services.

3. Secure Access Via Web Over Reliable Protocols.

3.1 Authentication.

As mentioned before, client authentication and trademark protection must be warranted. Both parts in the transaction have to be sure of the identity of the other part. This service is easily attained by the use of digital certificates.

This is a well-known subject in current open communications. The use of SSL (Secure Sockets Layer) protocol [3] can solve this problem.

Our prototype has a Secure Web Server to which the client is connected. The client can verify the server identity and be sure to whom he is asking for multimedia content. Identities are guaranteed throw digital certificates issued by an own Certificate Authority (CA).

On the other hand it is important to consider privacy. It should be impossible to anyone but the server to know what the preferences of the client are. So client anonymity should be provided if demanded.

Our system uses a block structure as shown in Figure 2. The server is implemented using the Apache web server [4] with modssl [5] module to add SSL services. Both packages are open source code. This server is configured to require client valid digital certificate (step 2 in Figure 2). So if the client is not an authorized party the communication

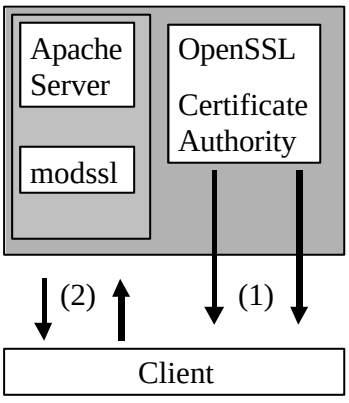

Figure 2 Server blocks diagram.

will not proceed.

The Certificate Authority is done by means of OpenSSL software [6]. The CA has the ability to issue two types of valid certificates (step 1 in Figure 2): actual identity certificates, in which client anonymity is not provided; and unidentified valid client certificate, in which only the authorization of the client is certified, not his identity.

Once the client has a valid certificate he can access the content database. Both identities (client and server) are checked by SSL protocol. Then, the service is chosen and the client will be asked for a payment. The Server Database was implemented using PostgresSQL [7] open source package.

3.2. Secure Payment.

The simplest scheme for secure payments consists of three parties: the seller, the buyer and the bank. See Figure 3. The buyer, the one who asks for a certain service and must pay for it. The seller who offers the service and will receive money for it and the bank (or financial institution), a third party from which the buyer's money is drawn and to which it is returned as seller's income.

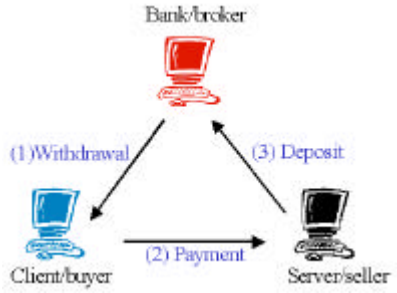

Figure 3 Simple Electronic Payment Scheme

Likewise, this scheme is divided in three actions: withdrawal, payment and deposit. According to the time when these actions take place the secure payment methods could be classified into pre-payment, instant payment and credit.

In pre-payment methods the money is drawn from the bank a priori. Instant payment stands for contacting to the bank at the same time the transaction is being carried out. In credit payments the client does not withdraw the money from his

bank account till some time after the purchase is done.

If the financial institution is contacted during the transaction, the payment is called on-line otherwise it is called off-line.

When electronic payments are considered, new features arise. In some cases it is desired that the client identity will remain anonymous. This seems a contradiction with identity guarantee, but can be overcome if we assure the client is an authorized purchaser although we do not know his actual identity.

When these new features are offered new threads appear: token forgery and double spending. The method must prevent anyone from being capable of issue a valid token (or electronic coin), furthermore a valid token (issued by the authorized entity) must not be used more than once. Usually, when such payment features are desired, tamper-proof devices as smartcards are used [8]

The Secure Payment method in SSADE project protects client identity (is anonymous) and warrants the seller to be paid for his services. It is also an off-line and pre-payment method. It avoids token forgery by using public key cryptography and hardware devices. It also prevents double spending by using spent-tokens databases. Instead of using smartcards, the SSADE payment method uses CD-ROM cards containing valid token and seller data. [9]

The payment scheme works as follows:

Withdrawal. When a web client wants to purchase for some multimedia content he will ask for a valid CD-ROM card containing different valid tokens. Each valid token corresponds to a coin of minimum service value. A token is made up of a serial number, a coin value and a site certificate. The card has a ciphered zone using the server private key and another one using the server public key. All this information is stored in the card using a passphrase revealed only to the purchaser when buying the card.

The passphrase protects the information in the card to be accessed from any other one but the purchaser. The server private key zone assures the purchaser that this is a valid card that could only be issued by the server. The server public key zone assures the server that this is a valid card that could only be issued by itself.

The card is not sold by the server but by authorized spending machines or brokers. Thus, the server does not know who has bought the card and cannot trace client identity. The money itself is contained in the card. Each token can only be spent in a particular server so the video-server itself can check if the token has already been spent. Not on-line checking with the financial institution is needed. The money is deposited into the seller account in the very moment the card is purchased. That means that loosing the card implies loosing the money, just like pre-payment phone cards.

Payment. Once the client has a valid card containing different tokens he can ask for a certain service via Internet browser (and secure web server). When service and client preferences are chosen properly, the multimedia server will ask the client to introduce some valid card in the CD-ROM reader. Then he will ask the client to introduce the passphrase that will allow the server to access the card content. This assures that the card will only be used by its actual owner. No card loss will lead to fraud unless the passphrase will also be lost. When the server reads the content of the private key zone it can be sure the token could only be issued by itself (cause he is the only one capable of ciphering with his private key). Then it removes the corresponding valid token serial numbers from his valid-tokens database, so the token will only be used once.

When all these steps are followed, the server sends to the client the data he will need to access

the multimedia stream. This stream might be ciphered in order to protect it from eavesdroppers.

Deposit. In this type of off-line pre-payment methods, the deposit is taken at the same time the withdrawal is done.

This payment method is patented under patent number 200002611 [9]

The most difficult problem to solve in this method was the fact that the Server might access the File System of the Client. Clients have to allow the Server to read from his CR-ROM reader. This is not a trivial problem cause most current technologies protects the client system from malicious actions by not allowing anyone but the client itself to access the own file system.

Fortunately, JAVA2 technology [10] allows fine-grained access to client resources by using a configuration file called Policy File. This gives us the ability to grant specific permissions to a particular piece of code about accessing specific resources of the client depending on the signers of the code and/or the URL location from which the code was loaded.

4. Data Confidenciality Over Unreliable Protocols

As we mentioned before, data should be protected from unauthorized third parties. This is easily achieved by means of symmetric ciphering. The inclusion of ciphering algorithms in multimedia communications is critical in terms of time. Cryptographic techniques must not add significant delay to data transmission or excessive packet loss due to time constraint violation will occur.

The SSADE project includes symmetric ciphering to the data stream, but it distinguishes between server side and client side due to its different hardware features and time requirements.

Files are encrypted on-line before sending in order to use different keys for each file, even during the same session, possibly changing the keys periodically.

Client Side. This is the less time restrictive side. On the one hand usually just one multimedia stream will be deciphered by a client, on the other hand it is important to the client to be as much universal as possible. This is why the client side was developed in JAVA language. This allows the client to be loaded via web by using the applet technology. This choice greatly simplifies the development of the client side since JAVA has a wide variety of cryptographic tools. The study and right election of the cryptographic tools of the client side was another important item in the SSADE Security Module. [11]

Server Side. Typically, a multimedia server can serve of the order of tens of video streams. This reduces at most the computational load that can be offered to the server. An optimized C programmed DES algorithm has also been developed in order to allow the server to cipher many different streams without having an effect over the total delay. This optimized version offers a throughput of 30Mbps over a 500 Mhz P-II [12]. AES was not considered since not JAVA cryptographic provider for the client side was available.

5. Conclusions and Future Work.

In this work we have presented the solutions adopted and the technology used in order to add security services to a video-on-demand server. This work was part of the SSADE project, *Secure System for the Access and Efficient Distribution of Multimedia-on-Demand Services.*

The goals of the Security Module were Secure Access, Anonymous Payment and Content Secrecy Protection. The first two services are performed over a communication phase using reliable transport protocol: TCP. Secrecy is achieved over a

communication phase using unreliable transport protocol: UDP.

SSL/TLS is used to warrant Secure Access and privacy to client preferences. The use of both client and server digital certificates is needed.

Anonymous Payment is achieved by means of a prepayment method consisting in a CD-ROM card bonus system. This payment method was patented.

Java client side technology was used to implement multiplatform client application. The server side was programmed in C programming Language.

Nowadays, we are working in the extension of this video server to multicast technology. Particularly, the session key distribution system has to be changed if multicast technology is used instead of unicast connections.

References:

[1] Multimedia Networking. Szuprowicz, B. Mc Graw-Hill, Inc. 1995.

[2] Secrets and Lies. Digital Security in a Networked World. Schneier, B. John Wiley & Sons, Inc 2000.

[3] SSL 3.0 Freier, Karlton, Kocher. Internet Draft. November 1996

[4] http://www.apache.org

[5] http://www.modssl.org

[6] http://www.openssl.org

[7] http://www.postgresql.org

[8] Sirbu, Marvin. Credits and Debits on the Internet. IEEE Spectrum. Feb 1997.

[9] Pegueroles J., Rico F. Procedimiento para realizar pagos a través de Internet mediante una tarjeta de pago basada en CDROM no circular. Spanish Patent Number 200002611

[10] Pistoia, M., Reller D.F. (et al) (1999), Java 2 Network Security 2nd Edition. Prentice Hall Inc.

[11] Arasa, Jose L. Estudi de la integració de confidencialitat en servidors de vídeo. Aplicació a tràfic real. Graduate Thesis. Director: Josep Pegueroles. 2002

[12] Rico-Novella, F. Sanvicente, E. Strengthened DES-Compatible DES for SmartCard Applications. SCI2000, Orlando. July 23-26 2000.