THOTH - A FRAMEWORK FOR BUILDING SECURE TV BROADCASTERS NETWORKS OVER THE INTERNET

Thiago Curvelo dos Anjos, Luiz Henrique Freitas, Guido Lemos de Souza Filho and Tiago Salmito
Digital Video Applications Lab, Federal University of Paraíba, João Pessoa/PB, Brazil

Keywords: Security architecture, TV content exchange, television virtual enterprises, security in collaborative systems.

Abstract: Nowadays satellite link are costly. Small TV stations can not afford such expenses and big TV stations make huge investments on such infrastructures. Instead of satellite, IPTV based technologies allow real time distribution of digital content with lower costs. Security is one of the main impairments for using IPTV on such type of applications. Considering security as a mandatory requirement we designed Thoth: a framework for creating secure virtual organizations platforms to share TV content among a scalable number of TV stations.

1 INTRODUCTION

The television is currently dominated by three distribution technologies: over the air broadcast, cable, and satellite. However, television industry is in the middle of profound changes caused by IPTV technology. IPTV provided by telecom service providers is starting to compete with existing broadcasting services via terrestrial, satellite and cable networks. The increasing demand for digital content, improvements on distribution and compression techniques in addition to high network bandwidth have made IPTV feasible

Many telecommunications companies are betting their future on the IPTV “Triple Play”: data, voice and video. “Data and voice traffic, delivered over the same IP pipe as video, can be more easily integrated with the viewing experience” (Wales et al, 2005). The use of an IP network to deliver content also makes it easier to provide new features.

Enterprises are now facing growing global competition and their continuous success in the marketplace depends on how efficiently the companies are able to respond to customer demands. The formation of virtual enterprise network is taking up momentum to meet this challenge (Lau, 2005).

Moreover, the idea of a dynamic organization combining synergetic efforts to perform a given business project is more likely to achieve costumer satisfaction and market needs than enterprises by themselves.

The combination of IPTV and Virtual Enterprises technologies create the perfect environment to develop new TV applications. In order to explore this opportunity we developed a framework that makes possible to instantiate secure platforms to share TV content among a scalable number of TV stations. This platform may be used to set up virtual TV networks formed by a set of individual broadcasters working together organized as a virtual enterprise. The framework we developed is called Thoth, and it was named after the Egyptian god that was responsible for production and dissemination of knowledge.

In order to properly work in a TV scenario, the software needs more than just achieve system functionalities, it must ensure data security.

The access to organizations’ resources is not public and must be restricted to a set of specific users. The first step is to ensure that users are authenticated before they use the system. However, authentication itself is insufficient to control who have permission to use the resources. Even legitimate system users can not have rights to perform all application functionalities. In addition, it is necessary to control which users have access to which resources.

The implementation of an authorization mechanism ensures that only users who have authority to do some task are allowed to do it. However, beyond access control, on business environment it is necessary also to register users’ actions, in order to make them responsible for their

Curvelo dos Anjos T., Henrique Freitas L., Lemos de Souza Filho G. and Salmito T. (2007).
THOTH - A FRAMEWORK FOR BUILDING SECURE TV BROADCASTERS NETWORKS OVER THE INTERNET.
In *Proceedings of the Second International Conference on e-Business*, pages 57-62
DOI: 10.5220/0002113500570062

acts. On TV environment, where copyrighted content flows among stations, this control must be carefully done due royalties' payments, for instance.

Another important concern regards security policy. The organization's security policy is a document which defines the organizational rules that must be followed in order to ensure a secure operation. These rules vary from one enterprise to another, because they have their own needs. Therefore, when it is necessary to design an application which will be used by many different companies, efforts to permit different implementation policies must be dispended.

Section 2 introduces a brief overview on Thoth architecture and functionalities. On section 3, security design is discussed and the Thoth security architecture is detailed. Section 4 exposes a case study of Thoth, applied to build a network of Brazilian TV Stations. Finally, in section 5, we present the conclusion of our work.

2 THOTH OVERVIEW

Thoth platform is a factory of TV Virtual Enterprises; it is used to create and also to provide support for the operation of distributed TV Virtual Enterprises. Thoth can be used to organize content exchange between a set of partner TV stations. The idea is to reduce content production costs by exchanging it, this way, a small television enterprise, instead of producing content 24 hours per day, can produce a smaller amount of it, to provide it for its partners on a virtual television network and use content provided by its partners to fulfill its daily programming.

Besides providing support for content exchange, Thoth can be used to build the television network reference programming schedule and to distribute this schedule of the TV network to every affiliate. Thoth broadcasts the content of the TV network schedule through the Internet using IPTV. It is important to highlight that this platform fits in the traditional television network scenario; where there is a main TV station (network head end) transmits content to its affiliate stations and then they retransmit it to end users adding its local content. Only authorized personal can share content on the network regarding copyright issues. In this section we explain Thoth architecture and features. Thoth architecture is presented in figure 1.

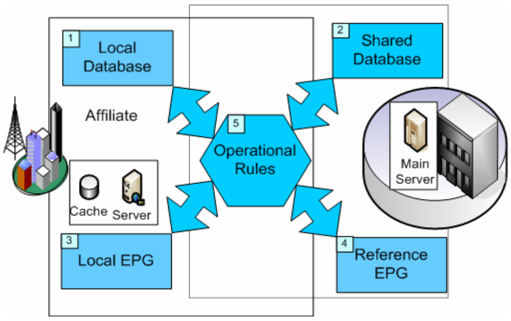


Figure 1: Thoth's Architecture.

1. All TV stations have their own database where they store local video content. The content in the database is used to build local Electronic Programming Guides (EPG). Video content on these databases are uploaded by authorized personal.
2. All TV stations have access to the shared database. They may download content from this database to build their local EPG.
3. In order to build local EPGs, programming operators from affiliate stations may use the video content from its local database, or from the shared database. In addition, some instances of Thoth have the option to use a reference EPG.
4. The main TV station builds reference EPGs with video content from the shared database and then sends them to affiliate TV stations. This EPG contains some empty time-spots that will be fulfilled by each station.
5. A set of operational rules that define processes and interactions in the architecture

The five entities mentioned in figure 1 forms the base of Thoth's architecture. However, in order to consider Thoth a factory of TV Virtual Enterprises, it has to achieve different requirements from distinct TV stations. These requirements may not be the same in different enterprises and sometimes they can be even opposites. Therefore, such requirements must be flexible and dynamically configured for each instance of a virtual organization. Thoth was designed to allow users to configure business rules, security policies and metadata.

This feature works on the so called flexibility functions of Thoth architecture, defining operational rules for the virtual organizations. By changing the configuration of theses functions, a new virtual enterprise with different rules is created. These flexibility functions are showed on figure 2.

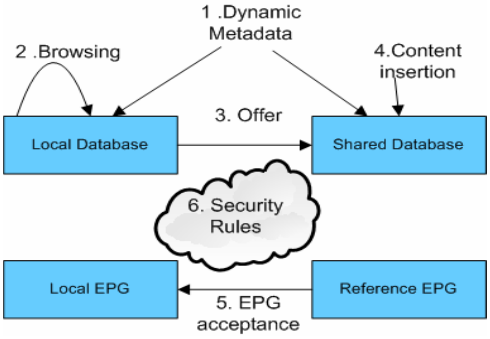


Figure 2: Thoth Flexibility functions.

1. Cooperation is a key aspect in the virtual enterprise paradigm (Camarinha-Matos, 2001). Because a virtual enterprise is built according to the changing business opportunity, the cooperative partners in a virtual enterprise may have different priorities. On Thoth, various users (TV Stations) may have different attributes requirements to describe their videos and the TV schedule. To give database's control to its administrators, a dynamic metadata approach was employed. Hence, each station is able to define and create metadata to achieve its internal requirements, without interfering on another station when offering or getting video.
2. In Thoth, affiliate stations can build their local EPG using video content from their database and from the shared database. However, improvements on video content exchange can be achieved by allowing users to browse and get content directly from other stations.
3. In order to advertise content to others stations, affiliate TV stations must either enable the feature presented above or offers this content to the main TV station. However, the offered content may be evaluated and accepted or rejected by the main TV station. Accepted videos are stored in the shared database and can be used by all stations. This flexibility function regards how the offering process occurs. We have got four different cases: (i) it can be disabled; (ii) it can be set to automatically accept an offer; (iii) every time an offer is made one person will evaluate the content; (iv) instead of one person, a council will evaluate the content using a voting system.
4. This issue regards how the shared database is populated. It may consist only by offered videos from affiliate TV stations, or only by uploaded video on the main TV stations or, in a third scenario, working with both cases.
5. The main TV station builds EPGs with video content from the shared database and then sends them to affiliate TV stations. However, the acceptance of this EPG by affiliate stations can be configured in three different ways: First, the acceptance is set to be optional, this ways affiliate stations may choose not to use the reference EPG (i.e. on a cooperative TV network). Second, the acceptance is mandatory and local EPG administrators are not allowed to change the schedule (i.e. on a hierarchical TV network), they are only allowed to add content on the unfulfilled spots on the reference EPG. Finally, the acceptance is mandatory but local EPG administrators can change the schedule, therefore, they can alter EPG as they want, however, they have to entirely broadcast the original content from the reference EPG.
6. In order to control users' access and to ensure only authorized personal perform the tasks, Thoth implements an authorization mechanism, where the organization security policy is defined and, for every user action, the right definitions are checked.

3 THOTH'S SECURITY DESIGN

On this section, we present the features of Thoth's security design issues.

So as to ensure quality of the adopted security solution, Thoth's design was based on the use of security patterns (Schumacher et al, 2006). Security patterns, like design patterns, consist in a set of generic, high quality and proven solutions to specific security problems. They are catalogued concepts, which have been applied successfully in the past over and over again.

An important feature within security design scope is transmission. All communication among station is done using security channels, a well-known pattern, employed to ensure confidentiality. To implement security channels Thoth uses the secure socket layer.

On the follow we discuss main features on security design.

3.1 Authentication and Identification

Authentication is the binding of a computer identity to a user (Bishop, 2002). When a user goes through the authentication process, and he is properly identified, a security session is created. A session is a large used pattern which consists in an object that holds user relevant data (Schumacher et al, 2006). The user client holds a session id (i.e. cookies on a browser) and presents it on every request. The main role of session is to identify the user, avoiding him to re-authenticate on every action.

In Thoth there are two levels of identification. In the first level, the user identifies him on his TV station, by using login and password schema. Thus, if his authentication succeeds and the session is created, he will be able to attempt to execute tasks on his station local resources.

The second identification level occurs when the user attempts to access resources beyond his station. For instance, offering a program to shared database or retrieving reference schedule. In Thoth, each affiliate station has its own users and its own security server (that will be better showed on distribution architecture in section 3.4); therefore, there is a need to identification on main station site. On these cases, because the session has local station scope, the user has to be identified on control station. In order to create another session, and avoid user re-authentication, a digital certificate-based authentication is done.

Using this approach, each affiliate station has a certificate emitted by control station which acts also as a certificate authority.

When a station attempts to access these resources, it presents its certificate to the control station, which creates a session for it. The affiliates are to main station, as the users are to its affiliates.

That certificate-based authentication approach is also used when an affiliate attempts to retrieve video content from another station local database. The affiliates exchange their certificates in order to recognize each other as members of the same TV network. This approach is called known partners (Schumacher et al, 2006).

3.2 Authorization and Access Control

Users have different access rights, and these rights must be checked before the application executes any resource request. So as to ensure that, Thoth adopts the reference monitor pattern (Schumacher et al, 2006). Reference monitor is an entity which intercepts all requests for resources and checks them for compliance with authorizations. Therefore, all user requests are addressed to reference monitor, that queries the security database, and allow or deny rights to do a task.

Also through the reference monitor, using a pattern called limited access, the user interface is customized according to user's rights. In this way, the reference monitor hides or display functionalities to the user.

In Thoth, the main resources are the schedules (local and reference) and databases (local and shared). Each resource has different set of functions and different interests and responsibilities are involved. Defining detailed rules requires a high level of granularity.

Aiming to provide the fine granularity authorization control for the organizations needs, Thoth uses Role Based Access Control model (RBAC) (RBAC, 2007). RBAC is a NIST standard which regulates access of user to resources based on their roles in an organization. The roles denote organizational functions which describe authority and responsibility assigned to a user. In RBAC, the access rights are assigned to the roles, according to the role needs. The roles are assigning to the users, according to their functions on the organization.

In order to ensure the policy independency, the access control mechanism must be implemented on an independent layer. In section 4.4 we present MACA, the middleware solution for access control adopted by Thoth.

3.3 MACA: Authentication and Access Control Middleware

MACA (MACA, 2006) is a solution for provide authentication and authorization service for legacy or under developing applications. It implements a contextual authorization model (MOTTA et al, 2003), which extends RBAC reference model.

A contextual authorization allows or denies access based on evaluation of rules, during an access attempt. These rules are defined in terms of environment functions or variables, available on context, in order to implement specifics access policies. Using contextual authorization enhances the granularity of access control, ensuring more flexibility to implement distinct policies.

MACA implementation is based on open standards to ensure interoperability. It's a scalable solution, which makes possible a centralized access policy administration, from different systems, for heterogeneous applications, made in different languages. Furthermore, in future their services will be available via web services, aiming to improve interoperability.

3.4 Security Architecture

In this section, we show Thoth's security architecture. First, the Logic Model shows the solution elements. In the follow, the Distribution Model expose where the elements are placed on TV environment.

The elements of Thoth security architecture are showed in Figure 3.

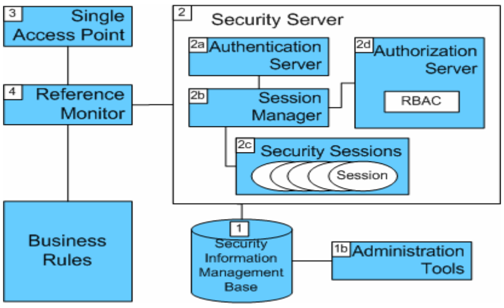


Figure 3: Security architecture: Logic Model.

1. Information about users, roles, resources and rights, used for authentication and authorization, are stored on a database known as Security Information Management Base (SIMB). The data on this base is populated and managed for system administrators using a set of Administration Tools (1.b).
2. The information on SIMB is retrieved by the Security Server, which is the main element of Thoth Security Architecture. It must ensure the security policy implementation.

   On the security server occurs the user identification through the authentication server (2.a). When a valid user attempts to log in on Thoth, the authentication server asks the session manager (2.b) to create a new session (2.c).

   The authorization server (2.d) is the entity responsible for verifying if users are allowed to execute the tasks they attempt to. The RBAC logic is implemented on this element. It checks user's permissions on the SIMB, based on his session.
3. All the integration between user and system is accomplished by a single access point entity. It is an element of the user interface that allows system access and it consists in a large utilized security pattern to provide a unique way access.
4. Finally, the reference monitor intermediates users and business rules. It is responsible for asking security server if the user has permission to execute a task, and allows or denies its execution. Reference monitor also asks for the user authentication when he attempts to log in.

Thoth architecture allows to implement distinct security policies without modifying business rules, therefore, making Thoth capable to easily adapt for different TV organizations realities. In the following section, the distribution model of Thoth architecture is exposed.

The entities of Thoth architecture are distributed among the stations affiliated to the television network. Figure 4 details the distribution model.

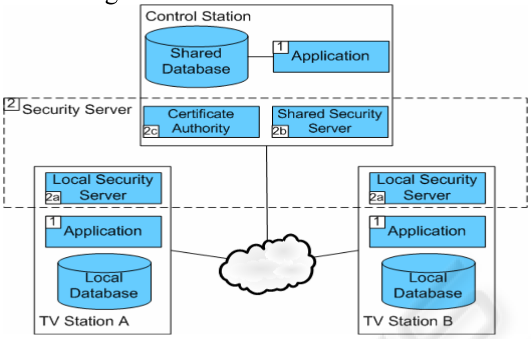


Figure 4: Security Architecture: Distribution Model.

Each station has an implementation of its business rules (1) and a local security server (2a). On the local security server, users are authenticated and authorized. However, when resources from the control station are required (shared base or main station EPG) both local and shared security servers are consulted. In these cases, the local server tests if the user has permission to do what he asks to, regarding his role. If a positive answer is obtained, the local server gets clearance with the control station and then, asks to execute the task on the control station.

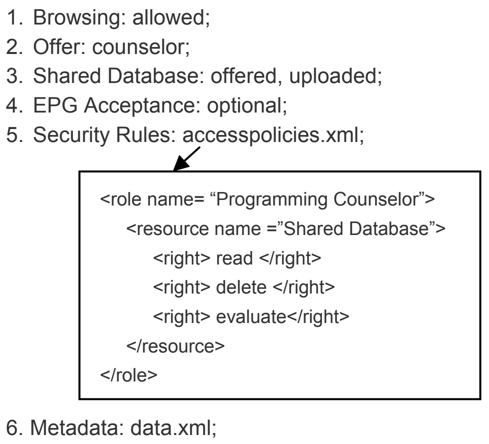
In the control station viewpoint, the affiliate stations are users, therefore, authentication is needed. So as to identify affiliate stations, the control station security server (2b) uses authentication based on digital certificate. Hence, control station acts as a certificate authority (2b), emitting certificate to the affiliate stations.

The use of this architecture for the distribution model makes Thoth security policy adaptability more flexible, because Control Station can regulate what their affiliate stations are allowed to do.

4 CASE STUDY: RITU

University TV Stations in Brazil spread scientific, technical and educational information throughout the country. However, a large number of these TV stations have limited budget and personal to produce such content and sometimes these productions are not enough to fulfill its daily programming content. In addition, video content produced by them is stored in only one place and at most times in non-digital Medias making difficult to share the content with other stations.

Brazilian University TV Stations are using Thoth to build a television network for sharing content aiming to complete their daily Electronic Programming Guide (EPG). This network is called RITU. RITU stands for Brazilian's university TV network for content exchange; from the Portuguese "Rede de intercâmbio de televisão universitária". RITU configuration is presented on figure 5.



```
1. Browsing: allowed;
2. Offer: counselor;
3. Shared Database: offered, uploaded;
4. EPG Acceptance: optional;
5. Security Rules: accesspolicies.xml;

<role name= "Programming Counselor">
    <resource name ="Shared Database">
        <right> read </right>
        <right> delete </right>
        <right> evaluate</right>
    </resource>
</role>

6. Metadata: data.xml;
```

Figure 5: Thoth configuration schema for RITU.

On RITU, there is one council that defines a reference programming guide and recommends it to the stations, however, TV stations are not contractually enforced to use this reference so, the acceptance of EPG from the Programming Control is not mandatory (4). Affiliate stations have complete control on its local EPGs; they can build their own programming guide with local video content, content from shared database or willingly accepting EPG from the RITU programming council.

Since RITU was developed for sharing content, affiliate TV stations have access to other TV stations databases and may download content from them (1). In fact, if a search is performed the showed results are from databases of all TV stations on RITU.

Another type of interaction among stations is the offer process; it always flows from the affiliate to the main station. At the main TV station the offered video content is evaluated by a one person (2). Accepted videos are stored in the shared database (3). In addition, video content can be uploaded by authorized personal; in this case the role responsible for uploading content is the Content Editor (3).

Moreover, there is a file describing the access control policy (5). It gives control to enterprises, allowing them to create and manage roles and rights, according to their needs. In figure 5 we used the role "Programming Counselor" as configuration sample.

Finally, there is a dynamic metadata system (6) where the user can define data according to enterprise needs.

5 CONCLUSIONS

Thoth is factory for TV virtual enterprises that uses IPTV to distribute video content among TV stations.

It inherits all the advantages of internet based applications like robustness and maintainability. It is a cheaper, more robust, and more efficient way to distribute content among TV stations.

In contrast of many distributed systems, where security concerns are neglected, Thoth focuses efforts on design a strong and flexible security approach. Its flexibility functions allow a high level of customization, supporting various TV scenarios. Thoth has been proving it very useful.

RITU, an instance of Thoth, help University TVs to complete their EPG, exchange content and minimize costs and flaws. It is a very powerful solution for TV stations to exchange and commerce their products with other TV stations.

REFERENCES

Bishop, M. 2002. *Computer Security – Art and Science*. Addison Wesley.

Camarinha-Matos L.M and Afsarmanesh Hamideh. 2001. Virtual Enterprise Modelling and Support Infrastructures: Apply Multi-agent System Approaches, in *Lecture Notes in Artificial Intelligence* LNAI Nº 2086, pp.335-364, Springer.

Lau, H., Chin, K.S, Pun, K.F, Ning, A. 2005. Decision supporting functionality in a virtual enterprise network, *Third International Conference on Information Technology and Applications (ICITA)*, Sydney, Australia. IEEE Computer Society.

MACA - Authentication and Access Control Middleware. In *http://maca.sourceforge.net*. Access in March, 2007

Motta, G. H. M. B.; Furuie, Sérgio Shiguemi. 2003. A contextual role-based access control authorization model for electronic patient record. *IEEE Transactions on Information Technology in Biomedicine*, New York, v. 7, n. 3, p. 202-207.

RBAC NIST Standard. In *http://csrc.nist.gov/rbac/*. Access in February, 2007.

Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Bushmann, F., Sommerlad, P. 2006. *Security Patterns – Integrating Security and Systems Engineering*. John Wiley & Sons, Ltd.

Wales C., Kim S., Leuenberger D., Watts W., Weinroth O. 2005. *IPTV – The Revolution is here*. University of California at Berkeley.