Security Aspects in Education Oriented Multimedia Networks

Juraj Londák[1], Pavol Podhradský[1], Peter Trúchly[2]
[1] Faculty of Electrical Engineering and Information Technology STU in Bratislava, Ilkovičova 3, 812 19 Bratislava, Slovakia
[2] Faculty of Informatics and Information Technologies STU in Bratislava, Ilkovičova 2, 842 16 Bratislava, Slovakia
pavol.podhradsky@stuba.sk

***Abstract* – The article summarizes security aspects related to multimedia networks with special focus to user identification, authentication and authorization procedures and mechanisms. Main stress is taken into account to the secure and flexible access of end users to multimedia contents, implemented on the application layer of the ICT architecture platform. The novel network architectures supported innovative educational paradigms "Student self-directed learning" based on "Student centric" model of education, is described in the paper. Practical part of the paper introduces application of modern multimedia network architecture, with the integration of the actual HbbTV concept in the heterogeneous ICT infrastructure, to provide on-line and off-line educational multimedia content to end users – students participating in the e/m-learning process. The Service Oriented Architecture (SOA) based on web services, a "distributed architecture that enables software components to be published as services over the Internet through a programmable interface and using Internet protocols for the purpose of the providing ways to find, subscribe, and invoke those services" [4]. The wide portfolio of the multimedia content and e/m-learning approaches and mechanisms are presented in the paper. The integration of the HbbTV concept to the heterogeneous ICT infrastructure, applicable for the on-line and off-line educational process is described in the paper.**

***Keywords* – Authentication; Autorization; Security; Multimedia Network; Student Centric Model; Distributed educational network**

I. INTRODUCTION

Over the last 20 years, the information and telecommunications systems achieved rapid development towards globalization and inter-dependence of applications and content delivery. This development is directed through the specialized business systems to households and the private sector in the form of multimedia content due to the ever-increasing popularity of the Internet.

A significant share of this development represents end-user terminals at an affordable price, from functionality point of view on a much higher technological level and with improved ease of use accessible to a wide range of people with different age groups and preferences.

The multimedia services provided over the last few years trying to adapt multimedia content with a range of interests of users based on their habits, preferences when searching for specific information on the Internet, friends around them and so on. Applications which was previously independent creates linked services.

This trend hit in the privacy of the user, especially concerning the handling of personal information and trust, where the boundaries are not always clearly defined and easily understandable to the user. The development of new multimedia applications, systems and their mutual entanglement of rules in the information security often perceived in different manners with regard to user privacy. It does not necessarily happen intentionally, but in order to provide users the service comfort and enjoyment from its use.

II. THEORETICAL BACKGROUND

Multimedia content security has a number of specific requirements that should allow to answer to the following questions:

Who has issued the multimedia content? Who is the content owner? When was the content issued? Who has access right to the content? Is the content modified? Where was the content modified? What was the original content before modification?

Security access policy is usually proposed to allow access only to authorized users whose identity was verified upfront. This process essentially consists of three distinctive steps, namely the identification, authentication and authorization.

1) Identification: is a step where user identify himself using token or identification chain, usually in the form of e-mail address or phone number.

2) Authentication: is the mechanism whereby systems may securely identify their users. Authentication systems provide an answers to the questions: *Is the user really who he/she represents himself to be?*

3) Authorization: by contrast, is the mechanism by which a system determines what level of access a particular authenticated user should have to secured resources controlled by the system. Authorization systems provide answers to the following questions:

- Is user X authorized to access resource R.
- Is user X authorized to perform operation P.
- Is user X authorized to perform operation P on resource R.

978-1-4673-9555-7/16/$31.00 ©2016 IEEE

We will focus more to authorization and authentication in next sections.

A. Authentication

Users can be authenticated using information based on different natures. They can be represented by following statements.

- Something you know: Knowledge factors include things a user must know in order to log in: User names, IDs, passwords and personal identification numbers (PINs) all fall into this category.
- Something you have: Possession factors include anything a user must have in his possession to log in. This category includes one-time password tokens (OTP tokens), key fobs, smartphones with OTP apps, employee ID cards and SIM cards.
- Something you are: Inherence factors include any biological traits the user has that are confirmed for log in. This category includes the scope of biometrics such as retina scans, iris scans, fingerprint scans, facial recognition, voice recognition.

In all three modes of authentication system and user shares agreed secrets (so called Authentication Key). User and system agrees on these secrets during registration. In the case of usage of biometrics mode (during registration), the system records digital representation of some aspects of the user's physiology or behavior.

It is possible to combine all three modes of authentication in order to improve security levels when it is required.

Multifactor authentication dramatically improves security. It is unlikely that an attacker could fake or steal all three elements involved in 3FA, which makes for a more secure log in.

B. Authorization

Access control models are used for the application of ~~the~~ rules for established safety rule and they define the conditions under which it is possible to access the resources of the system and its services. Currently there is several major access control models [1].

- **Discretionary Access Control (DAC)** allows the owner of the object define who can and who cannot accede to this object. This model is therefore sometimes called Identity-Based Access Control (IBAC).
- **Mandatory Access Control (MAC)** is used to determine what may be the subject (the user) to access. The subject can thus access all objects whose authority level is lower or equal than object classification.
- The most widespread model is the **Role-Based Access Control (RBAC)**. It uses roles and groups to grand the qualified entities rights to access object. The user can then access the object based on the role and group that has authorized. The great advantage of this model is that in the most cases it is sufficient to modify roles and group authorizations and not users itself.

C. Security protocols

Service integration of different systems is conceptually similar to the integration of services within a single system. Different requirements may ultimately lead to propose specific solutions. As the differences in security protocols, flexibility and security that require different services to interact, managed under different administrative domains. In a distributed system increases the importance of defining and standardizing interactions between services, message formats and content.

Addressing these issues through proprietary and closed solutions are cost ineffective and provides almost no opportunities to flexibly scale functionality and integration with other services in the future. Moreover, individual solutions cannot be re-administered in a different environment. For these reasons, it is common to rely on standardized security protocols.

Figure 1. Student centric model

1) Kerberos

Kerberos is an authentication protocol developed at the Massachusetts Institute of Technology (MIT) in 1980. Current standardized version is Kerberos v5.

Kerberos is an authentication system that allows the addition of Kerberos clients and services in real time through a central entity, referred to as the Key Distribution Center (KDC). [8]

Kerberos standard does not cover the process of building up a trusted relationship, this process is left to the administrator during system design. Kerberos has been proposed in order to provide encryption mechanisms for authentication in an insecure network. Protocol serves to protect the messages that are exchanged during the authentication procedure. All subsequent communication between the client and the service is no longer protected via Kerberos applications.

Kerberos is a protocol relying on TCP and UDP protocols. This protocol has still influence in design of new security mechanisms. However, it was proposed before security

978-1-4673-9555-7/16/$31.00 ©2016 IEEE

mechanisms such as TLS or HTTP and HTTPS. Therefore, it lacks popular functionalities widely used in multimedia applications today.

2) OAuth

OAuth is a protocol used for authorization and allows third party applications to obtain restricted access to a particular service, without the need for knowledge of the password.

OAuth is classifying native applications installed on the terminals as Confidential clients and Public clients, which are web applications. The great advantage of OAuth protocol is its relative simplicity and support of currently very popular web technologies such as RESTful design, JSON format as well as native TLS support [2].

However, OAuth specification does not address some important safety requirements. While the protocol addresses the problem of dynamic establishment of trust between the client and the central party providing OAuth. It does not cover recovering trust between the service and a central party. Protocol design assumes that the setting of trust between the service and the central party is made during the design phase manually and within the same domain.

OAuth also does not consider what should be done on the Central Party side, in case of changes related to the introduction of a new resource within the service.

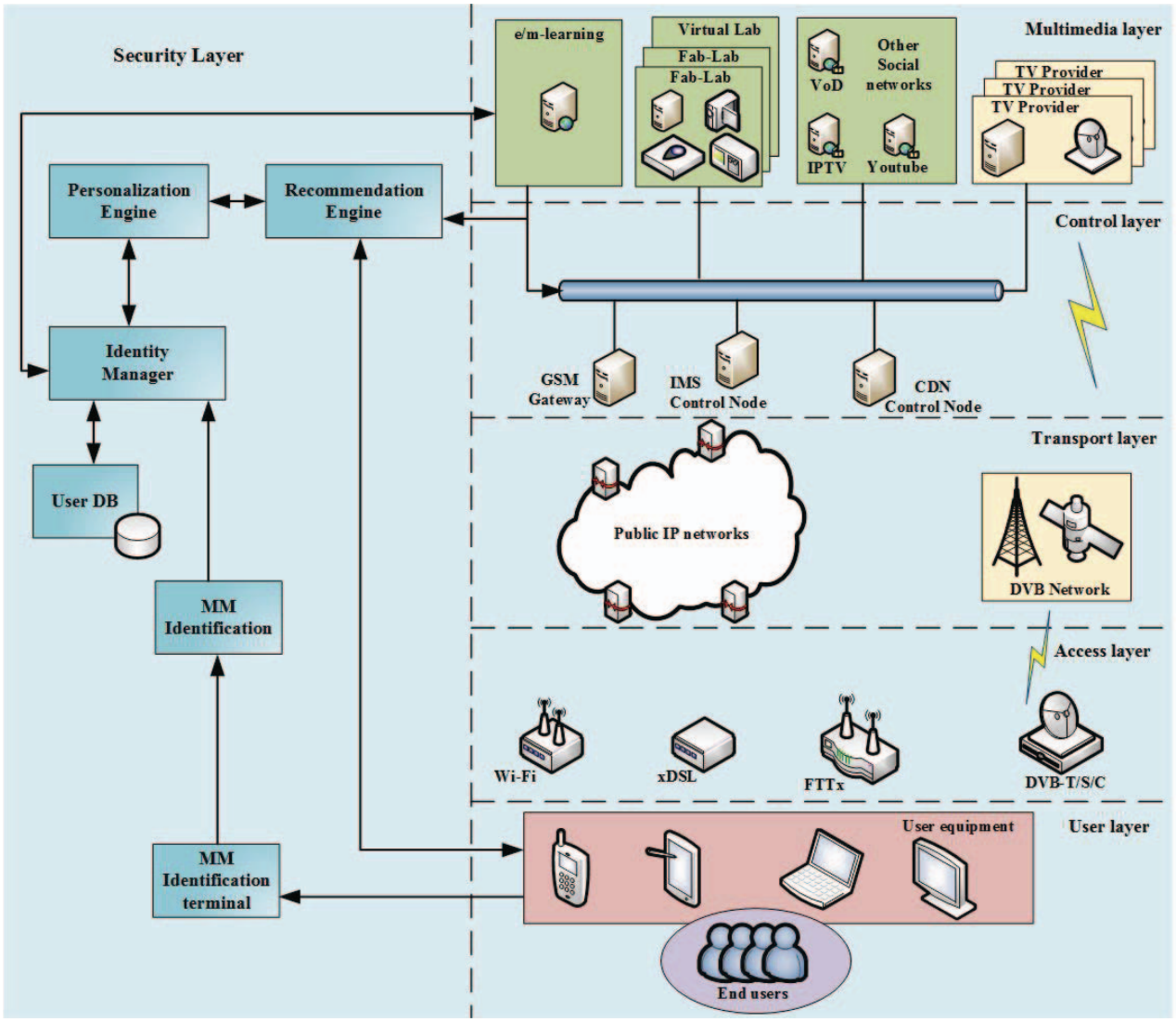

Figure 2. Distributed educational network

III. Large Scale Distributed m/e – Learning Platform

In the old paradigm the instructor is viewed as the only source of all the knowledge, everyone learns the same way, the class is the only place where knowledge disseminates and the course is the only way in which knowledge is transmitted. On the contrary, **the new teaching paradigm is dynamic and student-centric**. In this approach **the student acts as a performer that actively controls the flow and the amount of knowledge according to his/her specific needs**. [4]

Fig. 1 depicts the new student-centric teaching model our team is implementing and experiment with. This model allow the development of new skills based on emotional and social learning

IV. Distributed educational network

The proposed concept of the e/m–learning platform is illustrated in Fig. 2. The whole platform is designed in respect with a self-directed learning paradigm explained early in this paper.

The top layer of proposed platform is represented by multimedia layer which consists of applications providing multimedia content and other education resources and services to end users. It accommodates LMS system itself which integrates all services and sources to a one coherent portal. It also facilitates communication with Identity Manager and Personalization Engine. LMS provides possibility to enrich educational materials with multimedia content hosted on local services like IPTV or VoD subsytems or on public services like Youtube or Vimeo, Facebook, etc.

The platform is designed to be able to accommodate multimedia transport via not IP networks. Fig. 2 illustrates possibility to receive content via DVB-X networks witch is in line with intentions of incorporation of HbbTV architecture into educational platform. One of the advantages of HbbTV incorporation is possibility of multiscreen usage. In multiscreen scenario user it is allowed to use multiple devices to enrich his study experience. On the other hand it brings challenges to address multiscreen synchronization and A/V synchronization when one device receive content from multiple independent sources (example: video via DVB and Text via IP).

V. Secure Access to Multimedia Content

A. User Profile (Multilevel Identification / Autentification)

Multimodal identification allows detection of one or more users located in affected area [3], [7].

Identity manager is responsible for the management of information about users, devices and relationships between them. This includes items such as user ID, links to user profiles, authorization and authentication data and device ID. It is firmly connected to the user database which contains the user profile and related services.

B. Services/Applications Personalization

The personalization is responsible for providing personalized group profiles which are created based on individual user profiles. The module must obtain individual user profiles. Simple illustration of this functionality in education network could be situation when system reads each user's enrolled courses and group them into focus groups and provide them recommendation for future enrolments. Possibilities of used algorithms have much wider usage.

C. Recommendation Engine

Recommendation engine provides the functions of applications and services that can be recommended to end users. Engine offers study materials, courses and labs based on the user profile created by personalization engine.

VI. Conclusion

The security aspects related to end users access to multimedia content offered and provided via heterogeneous ICT network architecture are discussed in the paper. This process essentially consists of three distinctive steps, namely the identification, authentication and authorization of the user to have secure access to his/her personalized set of multimedia content (learning courses and lab experiments) based on his/her user profile.

The HbbTV network architecture ([5], [6]) extended by the e/m-learning subsystem and the subsystem of set of fab labs and virtual labs and also by further subsystems was used as the heterogeneous ICT infrastructure providing the wide spectrum of the multimedia learning content supporting the "Student Centric" model of education, which is one of the main idea of the running H2020 NEWTON project [4].

Acknowledgment

This paper presents some of the results and acquired experience from the following projects: FP7 research project HBB-Next, No. 287848, [5], [6], H2020 project NEWTON, No. 688503, VEGA project INOMET, No. 1/0800/16 and APVV project MUFLON, No. APVV-0258-12, [7].

References

[1] D. Cabarkapa, „Authorization Architecture for SWoT," AALTO UNIVERSITY, Espoo, Finland, August 2013

[2] D. Hardt a D. Recordon, RFC 6749, The OAuth 2.0 authorization framework, IETF Internet Engineering Task Force, October 2012.

[3] INOMET (Innovative of Multimedia Signal Processing Methods into Intelligent Systems and Services), national research project VEGA 1/0800/16, 2016–2018

[4] NEWTON (Networked Labs for Training in Sciences and Technologies for Information and Communication), H2020 projekt No.: 688503, 2016 – 2019

[5] Gómez Mármol, F., Rozinaj, G., Schumann, S., Lábaj, O., Kačur, J.: Smart AppStore: widening the frontiers of smartphone ecosystems. IEEE Computer, Jún 2014.

[6] HBB-Next (Next Generation Hybrid Broadcast Broadband), project FP7-ICT-2011-7, 2011–2014

[7] MUFLON (Advanced Multimedia Services in the Environment of ICT Future Networks), national research project APVV-0258-12, granted by Ministry of Education of the Slovak Republic, 2013 -2016

[8] L. Johansson, RFC 6880, An Information Model for Kerberos Version 5, IETF Internet Engineering Task Force, March 2013.

978-1-4673-9555-7/16/$31.00 ©2016 IEEE