AAA and Mobile Networks: Security Aspects and Architectural Efficiency

Nicolas Sklavos
University of Patras
Patra, Greece
nsklavos@ieee.org

Spyros Denazis
University of Patras
Patra, Greece
sdena@ece.upatras.gr

Odysseas Koufopavlou
University of Patras
Patra, Greece
odysseas@ece.upatras.gr

ABSTRACT
Security is a crucial factor in the provision of the network services, in both wireless and wired communications. Day by day, the number of subscribers is increased by an exponential function. Furthermore, the continued growth of network services, in addition to the available networks resources each time caused special needs for security and safety, throughout the transmission channel. Finally, billing services for network users is another crucial factor for the applied security mechanisms. AAA, or in different 3"A"s is a security standard which has lately been developed. The name of this standard (AAA) defines *A*uthentication, *A*uthorization and *A*ccounting services for the network subscribers. This work deals with the technical aspects of the three main security processes of AAA. In addition, an architectural model of this standard is also presented, from a generic point of view. Finally, key management issues are examined, which are applied in AAA.

Keywords
AAA, Authentication, Authorization, Accounting, Networks Security.

1. INTRODUCTION
One of the greatest challenges in the field of networks is to support the adequate security services for the supported communications and provided services [1]. Especially in wireless networks, the popularity of mobile devices increases rapidly due to the technology that allows users to connect to a network or to a domain, by anybody, at anyplace and at any time. Of course such actions tend to be real trends for the usage of networks and especially of internet available services, where economic aspects play the major role. Moving on this direction, it is proven a fact of major importance to support security capabilities for both users and networks providers, via software or hardware approaches [2].

MobiMedia'07, Month 8, 2007, Nafpaktos, Aitoloakarnania, Greece.

Starting with an authentication and an authorization processes during the initialization phase, network devices are allowed to gain access to both network services and data resources. Besides that common types of security, special needs for authorization are needed due to additional requests for access of sensitive network resources and possible billing services of the network provider.

It is obvious, that in our days there exist special needs for authentication, authorization and accounting for the network services of any kind, and especially for the billing ones. These security purposes are fulfilled with the AAA Standard [3]. AAA architecture and infrastructure, has been defined and standardized by the Internet Engineering task Force (IETF) and Internet Research task Force (IRTF) [4], [5], [6].

This work is dedicated to the *Authentication*, *Authorization*, and *Accounting* (AAA) Standard. First, each one of the supported security services is presented separately. Technical aspects of authentication, authorization and accounting are given, as well as security models for each one of them. Furthermore, a generic architecture of AAA is discussed. The basic idea, besides AAA generic architecture is that the three security services must be supported by the same security server. The architectural model, with the basic fundamental elements, is presented. Besides that, additional security schemes, such as key management, are presented. Especially for the key distribution, a three party security model is used as a real example of network transaction.

This work is organized as follows: Section 2 presents the Authentication Process of AAA. Authorization is described in detail in next Section 3. The next section is dedicated to Accounting. A generic architectural example of AAA is described in Section 5. Key Management issues are discussed in following Section 6. The paper finally concludes in Section 7, with conclusions and outlook of this work.

2. AUTHENTICATION PROCESS
Authentication is a process of two different actions: provision and verification [7]. For the transmitted information, an authentication mechanism must provide an electronic evidence of authenticity, as proof for the data procedures [8]. In the second phase, this proof must be verified. The two different actions of authentication are critical security mechanisms, which are needed for the secure access to networks, for both servers and clients.

In most of the cases, in order for the clients to gain access to the network, they must present their identity, besides some credentials.

The network is responsible for the verification of the stated identity of a certain client. The same authentication idea follows up network subscribers, common users, as well as network devices, when access to the network is the selected action. It has to be mentioned that there are cases where user authentication is different, compared with the device authentication, and must be performed separately. In these cases, the network operator must verify that both the user identification and the device also, are authentic. The authentication (security) process may need more than once, both user and device authentication, in a set of steps of a network access. Common certificates or cryptographic keys could serve both purposes. Passwords or ID cards could also be used for the same process, in cooperation with a security mechanism.

The most common architectural model for authentication is the Two-Party Authentication Model (Fig. 1). It is used when two nodes, a client and a server, communicate with each other without any middle third party, such as a gateway, or a proxy. The client has to authenticated, in order to gain access of the server. For this purpose a key exchange mechanism is applied between the two parties.

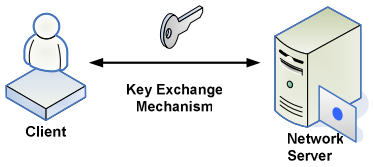

Figure 1. Two-Party Authentication Model

Due to the great number of users wishing to have access to a network and in addition to the network size, the Two-Party Authentication Model has been modified to include three parties (Fig. 2), in order to serve authentication in a more sufficient and satisfactory way. The user requests access to the network. The Network Access Server (NAS) acts as an AAA client and asks for the clients access permission. The authentication server (AAA Server in Fig. 2) is the real authority concerning the user access. AAA server operation is based on information databases, regarding users names, verifications etc.

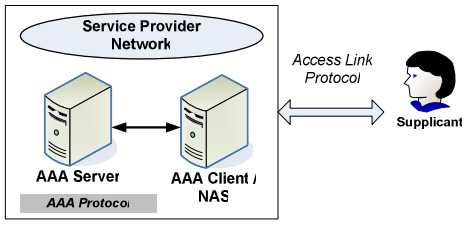

Figure 2. Three-Party AAA Authentication Model.

3. AUTHORIZATION

Authorization refers to the second A of "AAA". In most of the cases, authentication refers to the permission based on credentials, in order a user to have access to a network provider. Today, in many networks the authentication mechanism is quite enough for network access. Although there are several occasions, where the subscribers want to use alternative quality of service (QoS) capabilities. In this case, typical user verification is proven insufficient for the requested services and additional mechanisms must be applied. The network must take care of the subscriber consult entities, control additional parameters and finally permit or not the access to the requested service.

In fact, when a standard is specified, authorization is a procedure to which the least attention is paid. This is due to the fact that authorization is based on the security primitives of authentication. Although, based on the big difference between authentication and authorization, authentication subgroups are formed, in order to take care of authorization procedures. For example, we refer to the AAA group for Internet Engineering Task Force (IETF), which formed the Authorization Subgroup, responsible for the authorization [3], [5].

In the next Fig. 3, an architectural example for implementation of authorization is illustrated. The User sends a request for permission for service. The user's profile (UP) is stored to the Authentication Server. The Service Provider decide, upon to the UP, if the user is determined to use the requested resources or not. The decision is often based on a policy framework, which has been previously set. This framework contains different several architectural elements: policy repository, policy decision points, etc. A typical policy framework contains information in the policy repository such as: i) available services, ii) offered resources upon authorization, iii) authorization decisions rules, iii) vent logs, also for authorization. It has to be mentioned, that the policy information are managed and shared with other entities, inside the network. AAA server interacts with these entities, in order the right authorization decisions to be taken. The AAA server is allowed to retrieve the policy, for the authorization process.

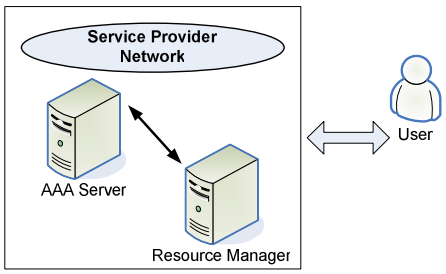

Figure 3. Architecture of Authorization Model

In the example of the previous Fig. 2, authorization follows the authentication process, and it is performed only in the case the authorization procedure of user's identity has been verified. The same server takes care of both authentication and authorization procedures. In the above architecture this is the AAA (Authentication, Authorization, Accounting) Server, which also performs the accounting process. The Service Provider Network administrates the Resource Manager. In the above model the Recourse Manager supports the provided services of the network, that the User May request.

4. ACCOUNTING PROCESS

Last but not least, AAA also supports Accounting Process [9], [10]. Accounting is a more complicated sense than the word defines. In general term, accounting defines all the information collected for the resources usage of a network. Subscribers of the

networks services and resources use them for a specific period of time, or for specific purposes. This service and resource allocation is translated to consumption, which is finally counted by this process, according to the applied accounting protocols. These protocols have security and reliability requirements for the billing services. The major applications specified for the purposes of accounting are: auditing cost allocation and trend analysis [11], [12], [13].

The interactions between the network devices, the accounting servers and the billing servers define the accounting management. Figure 4 illustrates the interactions of the various entities for the accounting process.

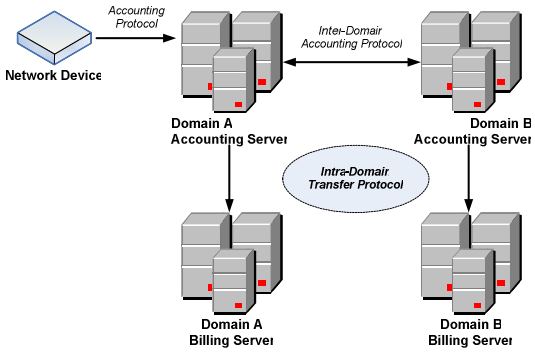

Figure 4. Accounting Management Architecture

For the Accounting Server the events between the inter- and the intra- domain differ and it manages them in an appropriate way. Inter-Domain accounting refers to the monitoring of services of an administrative domain, which are used within another administrative domain, B and A respectively in our case. Accounting packets and session records are needed to cross among the administrative boundaries. The other way of usage, Intra-Domain, defines that the services are processed in one administrative domain. In this case, accounting packets and session records do not need to cross through the administrative boundaries.

In the accounting process, there are potential needs for security, regarding both accounting policies and records. Secrecy is the major issue. Unauthorized users must not be able to read or modify accounting records and policies. In the next step, it is required that accounting data are the original ones. In this direction digital signatures could be used for the verification of the source authentication. Integrity is also major factor of security. Accounting data must no be modified or replaced due to their transmission throughout the network. For this purpose, digital signatures could also be used.

Finally, special care must be taken care of the accounting data. This means that the subscribers must verify that the billing regarding the accounting data is correct. There could be cases in which accounting data or billing has been measured in a fault way, due to bad configuration etc. A trusted third party could be used, in order to serve for the accounting billing data verification, between the accounting process and the network users.

Lately developed approaches, such as prepaid cards, tries to provide a hybrid solution for authorization and accounting, which could be performed at the same time.

5. ARCHITECTURE EXAMPLE OF AAA

In the following Fig. 5 the generic architecture FOR AAA is presented, RFC 2903 [6]. The AAA Architectural model implements an interaction between the User, the Application Module, and the Server (AAA). Authentication, authorization, and accounting processes are performed by the same AAA Server. AAA architecture interacts with other management entities, which provide the services and the functions. The last could be: mobility services, QoS, and bandwidth management.

The services are characterized by application specific information (ASI), which is controlled by the Application Specific Module (ASM). The policy rules are applied through the Policy Repository. There rules vary, from the AAA Server to Policy repository to AAA Server – ASM interactions.

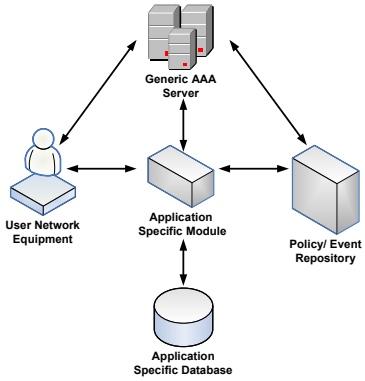

Figure 5. AAA Architectural Model

The generic AAA Architecture operation is based on a set of processes that are performed, in order a secure communication to be established.

First, a user request for authentication or authorization is accompanied by set of credentials. Then, the request is forwarded to the AAA server.

The AAA server, based on the sent credentials, verifies or not the user request for authentication. For this purpose, the server cooperates with the users' database records, as well as with the policy repository. The server continues to a possible authorization request, only in the case of successful authentication. The server is not required to have application-specific knowledge. For these reasons, server is able to refer to ASM. In different words, the tasks are divided between the AAA server and the ASM. In order this approach to be applied, ASI is needed to be separated from the authorization procedure scenario.

When the authorization request is determined, the server use additional rules from policy repository and takes an authorization decision. This is proceed, by the server even in the case that policy decisions or management are performed by other entities.

Finally, the Application Specific Policy Module is informed for the authorization by the server. Additional information could be provided for the requested service establishment. At the end, accounting reports on the server are recorded.

6. KEY MANAGEMENT

Key management is the responsible scheme for the generation, distribution, control and storage of the used cryptographic keys [14]. All the previous processes are applied to both secret and

public keys, and in many cases to key certificates. These services could be characterized by: applied encryption algorithm, key size, key management policies, and key established schemes. Key management procedure is closely combined with the one of the authentication. In most of the case, key issues of a secure communication have to be established in conjunction of the authentication procedure.

Extensible Authentication Protocol (EAP) [14], provides a generic authentication process. It can support alternatively many authentication procedures, while it could also be used as a key management framework at the same time.

In a Three-Party Authentication Model (Fig. 2), the peer (user or device) sends an access request, through the authenticator. This request is forwarded to the AAA server (backend authentication server), though the authenticator. The verification of the authentication is finally been proceeded in the AAA Server. The described process is presented in Fig 6. The secure communications of both peer-authenticator and authenticator-AAA server, are established based on key management issues controlled via the AAA server.

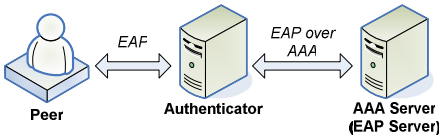

Figure 6. EAP Key Management Scenario

Key management for a Tree-Party Model (Fig. 2) is based on three different phases, which could be described from the diagram of Fig. 7. During "Discovery Phase" (phase a) the peer recognize the authenticator and take the knowledge of the communication parameters such as applied technology, security algorithms, and technical aspects like bandwidth rate etc. Authenticator here acts as a pass-through, and could not trust peer and vice versa, during this phase. Authentication process follows as phase b. An EAP Handshake is started between the peer and the network, through the AAA protocol messages. During this phase, authentication is combined with the derivation of keep materials, between the peer and the EAP server.

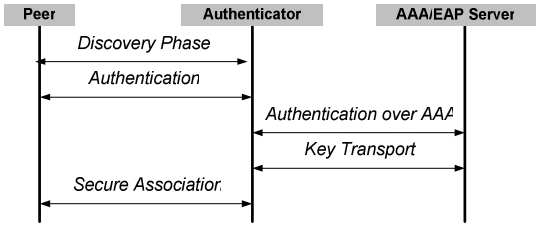

Figure 7. EAP Key Management Process

Additional keys must be generated, since the handshake conversation, between the peer and the EAP server must be protected. For this purpose transient EAP keys (TEK) are used. The EAP key management scenario is continued with the Key transportation, which refers to the key materials transportation from and to AAA server. After this process a secure association could be established.

7. CONCLUSIONS & OUTLOOK

Security is a primary requirement of any network, with wired and or wireless infrastructure. The specific needs for data transportation and especially for sensitive networks transactions have triggered the special needs for security and safety. AAA is a security standard that supports authentication, authorization and accounting services.

This work deals with the supported security services of AAA, in technical detail. In addition, a generic architecture for AAA is presented. Additional security schemes, such as key management, are presented and discussed, as far as they concerned in this security standard.

8. ACKNOWLEDGMENTS

This work is funded by Phosphorus IST Research Project. Contract Number FP6-2005-034115.

9. REFERENCES

[1] W. Stallings, *Cryptography & Network Security: Principles and Practices*, 4th Edition, Prentice Hall, 2006.

[2] N. Sklavos, X. Zhang, *Handbook of Wireless Security: From Specifications to Implementations*, CRC-Press, A Taylor and Francis Group, 2007.

[3] J. Vollbrecht, et al., "AAA Authorization Framework", IETF, RFC 2904, August 2000.

[4] J. Vollbrecht, et al., "AAA Authorization Application Examples", IETF, RFC 2905, August 2000.

[5] S. Farrell, et al., "AAA Authorization Requirements", IETF, RFC 2906, August 2000.

[6] C. Laat, et al., "Generic AAA Architecture", IETF, RFC 2903, August 2000.

[7] J. Vollbrecht, et al., "AAA Authorization Framework", IETF, RFC 2904, August 2000.

[8] J. Vollbrecht, et al., "AAA Authorization Application Examples", IETF, RFC 2905, August 2000.

[9] B. Aboba, et al., "Introduction to Accounting Management", RFC 2975, October 2000.

[10] S. Hares, and D. Katz, "Administrative Domains and Routing Domains, A Model for Routing in the Internet", IETF, RFC 1136, December 1989.

[11] P. Calhoun, et al., "RADIUS Accounting Interim Accounting Record Extension", draft, January 1998.

[12] T. Zseby, et al., "Policy Based Accounting", RFC 3334, October 2002.

[13] M. Beadles, and D. Mitton, "Criteria for Evaluating Network Access Server Protocols", IETF, RFC 3169, September 2001.

[14] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, "Extensible Authentication Protocol (EAP)", IETF, RFC 3748, June 2004.