A new Accounting Mechanism for Modern and Future AAA Services

Alexandros Tsakountakis, Georgios Kambourakis, and Stefanos Gritzalis

Abstract Accounting along with Authentication and Authorization comprise the concept of AAA provided by IETF (Internet Engineering Task Force). In heterogeneous environments, where different administrative domains and different wired and wireless technologies are utilized, those principles are often hard and complex to correctly implement and evaluate. Specifically, accounting which is our topic of interest, is in many cases a complicated procedure since many aspects need to be taken into consideration. In this respect, a distributed, flexible, robust, secure and generic accounting system needs to be implemented in order to provide the ability to determine which user has acquired which services and for how long at each operator domain. This work examines different scenarios applicable to such 3G/4G hybrid mobile environments and suggests a novel, generic mechanism to support accounting.

Key words: AAA, Accounting, 3G/4G Environments, RADIUS, DIAMETER

This paper is part of the 03ED375 research project, implemented within the framework of the "Reinforcement Programme of Human Research Manpower" (PENED) and co-financed by National and Community Funds (25% from the Greek Ministry of Development-General Secretariat of Research and Technology and 75% from E.U.-European Social Fund).

Alexandros Tsakountakis · Georgios Kambourakis · Stefanos Gritzalis
Laboratory of Information and Communication Systems Security, Department of Information and Communication Systems Engineering, University of the Aegean, Karlovassi, GR-83200 Samos, Greece, e-mail: {atsak, gkamb, sgritz}@aegean.gr

Please use the following format when citing this chapter:

Tsakountakis, A., Kambourakis, G. and Gritzalis, S., 2008, in IFIP International Federation for Information Processing, Volume 278; *Proceedings of the IFIP TC 11 23rd International Information Security Conference*; Sushil Jajodia, Pierangela Samarati, Stelvio Cimato; (Boston: Springer), pp. 693–697.

1 Introduction

Once a user successfully authenticates with the network and gains the appropriate authorization privileges she is granted access to network resources. From that time on, the user activities need to be constantly tracked and metered, in order for the network operator to calculate and accordingly charge the user. This procedure is called accounting. The main purpose of the accounting procedure is to bind user-related activities with accounting data. The latter may be the time spent connected to the network, the Kilobytes of data downloaded, or even some pre-defined tariffs correlated with a specific service.

The idea of AAA services has been under constant study and attention by researchers especially the last few years. However, as far as accounting is concerned, little work has been conducted as researchers mostly focus on the Authentication/Authorization functions and on security considerations of AAA architecture [1, 2, 3]. Accounting is considered straightforward and the IETF draft [4] directions are followed by all implementations. Most studies in the literature so far propose accounting systems that build on standard AAA protocols like RADIUS and are suited for specific environments and technologies [5]. At the same time these schemes usually rely on predefined number of users and relationships between those users and existing network providers [6, 7]. In our opinion though accounting should be performed in a more generic way thus avoiding the limitations stemming from the underlying network technology or the specific AAA protocol being utilized.

The rest of this paper is organized as follows. Section 2 covers some important background aspects of accounting in greater detail. In section 3 the requirements of the new accounting mechanism are presented and the analysis concentrates on the description of the proposed architecture. Last section offers concluding thoughts and future directions for this work.

2 Accounting

In a typical accounting scenario several entities are involved. First the customer who holds a subscription with a network operator who is responsible for offering and supporting network access to his customers. That operator is called the Home Operator (HO) and is the only party holding a user profile, consisting of detailed information regarding the user as well as the user SLA (Service Level Agreement). An external or foreign network operator may be utilized in case of roaming to allow the user to continue network access outside the Home Operator's covered area and is called Foreign Operator (FO). In most cases an FO holds a roaming agreement with the HO. The last party involved is called Foreign Service Provider (FSP) and is actually a third party capable of providing add-value services to users requiring them. These services are in most cases charged separately, but the cost is added to the cost of network access. Figure 1 shows all participants in an accounting scenario along with the connections between them.

Accounting can be a relatively straightforward process or become highly complicated as more and more network operators and service providers are participating in. The factors affecting the accounting procedure are bipartite. On the one hand lay the different administrative domains the user visits during vertical hand-offs. Whilst on the other emerge the technological variations, as more and more different technologies are available to the user.

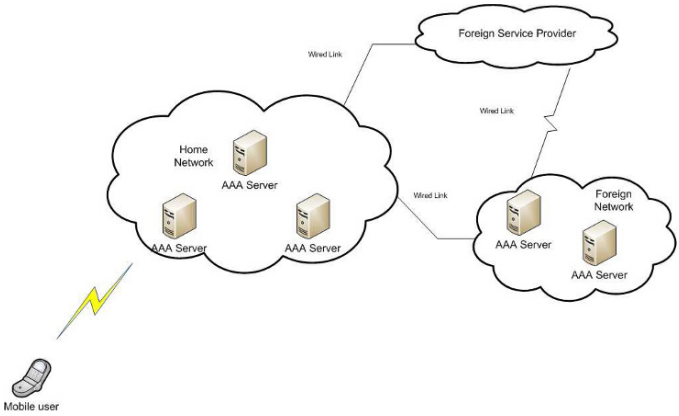

Fig. 1 Generic AAA Network architecture

In this respect, technological hand-offs and administrative domain hand-offs often become intertwined as the user enjoys the benefits of the new heterogeneous environments and their services, which in turn are derived from the use of innovative network technologies. Thus, modern accounting systems need to meet and satisfy several challenges and demands in order to provide robust and foolproof services to network operators.

3 Accounting architecture

3.1 Architecture requirements

Every new accounting system should take into consideration all the parameters related to: (a) the heterogeneous environment, (b) the multi-network operator relationship model, (c) the existence of many innovative technologies frequently incompatible and (d) the large number of mobile user population. In a nutshell the desirable requirements a new accounting system must meet are the following:

- **Generic.** The new accounting system should be applicable regardless of the underlying network access technology used.

- **Distributed.** The magnitude and complexity of current accounting demands can only be tackled with distributed architectures that mitigate future problems and technical failures.
- **Secure.** Data privacy, confidentiality and integrity should be ensured. Of utmost importance is the protection of user personal information. Private personal data should be safely stored and never be transmitted to any party other than the one the user has a contractual relationship with. At the same time accounting data regarding a user should securely and reliably travel between administrative parties.
- **Transparent to users.** Users must receive one single bill regardless of the number of operators or other charging parties involved in the process of accounting.

3.2 Proposed Architecture

According to our model during the accounting process an AAA Server can take either the role of the Root Server or the Administrative Server. The Root Server is an AAA Server inside the HO the user first attaches to. From now on, in terms of Accounting, the Root Server will be responsible for that specific user and will be used for collecting accounting events throughout the entire user session within the HO. The Root Server initializes and terminates the accounting process. Upon granting network access to the user the Root Server creates a unique identification number (ID) and stores a record mapping the newly created ID with the actual user. The actual user ID may be the user's International Mobile Station Identifier (IMSI) or Network Access Identifier (NAI). The first ID that the Root Server creates is called Master ID and is only altered, updated or deleted by the Root Server. Finally, the Root Server is responsible for the preparation of the final invoice to be sent to the subscriber.

The Administrative Server is initially the same as the Root Server. As the user moves, hand-offs occur and the user may need to attach to a different NAS Server or even require the services of a new AAA Server. Consequently, the Administrative Server is the local AAA, which is at the given moment responsible for the user. It is important to note that the Administrative Server can be an AAA Server that is located in the administrative domain of a foreign network operator. The administrative Server keeps track of where the user is physically located and thus minimizes data transfer requirements and bandwidth allocation for accounting purposes. This server is responsible for collecting accounting records while the user remains under his surveillance. Each Administrative server holds only limited information about the actual user, keeping only the required SLA information needed for charging as well as a reference to an ID (Master ID) sent to it by the previous Administrative Server.

Each time the user initializes an event that needs to be tracked the Administrative Server will create a new unique ID (called Event ID) mapped to that event. The Server will securely store in the corresponding database the correlation between the newly created Event ID and the received Master ID as well as the correlation be-

tween the Event IDs with accounting data. When a user leaves the current Administrative Server, or when required for other purposes, all accounting data gathered will be sent to the Root Server. The Root Server will eventually combine all events and store a single record for each user.

In case the user moves to the domain of a FO the same principles apply but the Master ID sent to the new Administrative Server inside the FO (by the Administrative Server inside the HO) is now an Event ID created by the Administrative Server in HO. The current Administrative Server takes the role of the Root Server inside the FO. When the user leaves the domain of the FO all the engaged Administrative Servers will send the relevant accounting data to the Root Server, which forwards them back to the corresponding Administrative Server inside the HO. That server will later send them along with its own collected accounting data to the Root Server in HO. If a FSP interferes, the current Administrative Server will allocate an ID to be mapped with the accounting data sent by the FSP.

4 Conclusions and Future work

The proposed accounting system is generic, provides secure means to transfer and store sensitive data, is distributed thus mitigating network failures and most importantly does not rely on, or affect by any means, existing technologies or protocols. On the contrary, it can be easily incorporated into the network operator existing mechanisms regardless of the underlying network technology. At the same time this generic behavior allows for interoperability between different network operators and service providers. The next steps of this work include the implementation and evaluation of a prototype system. DIAMETER will be used as the AAA protocol in charge and the test-bed will include both wireless and cellular networks.

References

1. Kim, H., Afifi, H.: Improving mobile authentication with new AAA protocols. Communications, 2003. ICC '03. IEEE International Conference.
2. Perkins, C.E.: Mobile IP joins forces with AAA, Personal Communications, IEEE,Volume 7, Issue 4, Aug. 2000 Page(s):59 - 61(2000).
3. Meng, Fang, An, Changqing, Yang, Jiahai: Implementing a Secure AAA System in IPv6 Network Communication Technology, 2006.
4. Authentication, Authorization and Accounting services, http://tools.ietf.org/wg/aaa/
5. Lopez, R.M., Perez, G.M., Gomez Skarmeta, A.F.: Implementing RADIUS and diameter AAA systems in IPv6-based scenarios, Advanced Information Networking and Applications, 2005.
6. Janevski, T., Janevska, M., Tudzarov, A., Stojanovski, P., Temkov, D., Stojanov, G., Kantardziev, D., Pavlovski, M.; Bogdanov, T., Interworking of cellular networks and hotspot wireless LANs via integrated accounting system, Wireless Internet, 2005.
7. Chaouch, H., A new policy-aware terminal for QoS, AAA and mobility management, International journal of network management.