# UNIVERSAL AUTHENTICATION FRAMEWORK
## *Requirements and Phase Design*

Jan Hajny, Tomas Pelka and Petra Lambertova
*Department of Telecommunications, Brno University of Technology, Purkynova 118, Brno, Czech Republic*

Keywords: Authentication, Authorization, Accounting, AAA, Security, Protocol, Access, Control, Mobile, Networks.

Abstract: The paper deals with the area of user Authentication, Authorization and Accounting (AAA) in computer networks. The current state analysis together with main trend identification is presented in the first part. These data are used as an argument for a statement about insufficient flexibility and security of nowadays solutions. As a reaction we provide a Universal Authentication Framework which should solve these identified issues. Our ambition is a good support of a wide range of devices – from mobile nodes like sensors, PDAs and mobiles to work stations and servers. We chose a modular platform for this goal to obtain sufficient flexibility which allows using any todays protocol together with possible future protocols. There is a basic structure description and operation phase description in our paper. We also provide information about new protocol inclusion. This paper also works as a starting document for further work and system implementation.

## 1 CURRENT STATE

The first phase of our research mainly comprised current state analysis in the field of AAA (Authentication, Authorization and Accounting). The goal was to find out whether today's solutions reflect a rapid change in the computer network domain and eventually find techniques or tools usable in a future authentication framework. Our starting point was a pack of more than 90 research papers and publications dealing with AAA systems. We analyzed these papers to learn overall image about directions in the present research. These directions can be illustrated by the Figure 1.

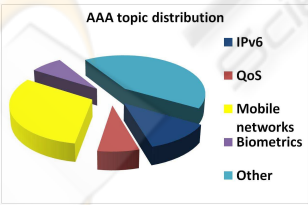


Figure 1: AAA topic distribution.

It is obvious from the mentioned graph that research groups are very often focused on mobile and wireless networks (right after unclassifiable topics). Many scientific publications discussed technologies connected with consolidation of wireless computer networks (like Wi-Fi) and mobile PLMN networks (Public Land Mobile Network). Another finding is that most of core techniques identified during our study are well–established but quite old. There are not many new findings in the AAA area and if there are then they usually improve operational parameters or data structures (Lee, 2007), (Jiann-Gwo and Cinhg-Song, 2007). Simply by thinking only on parameters of a new network and its efficiency the designers forget the security. They even simplify security procedures to eliminate time delays or to support weaker hardware devices. This activity has also an impact on AAA services – we can see a transfer from the 4-way handshake to the 3-way one or a replacement of PKI by simple challenge–response. Another discussed topic is a system modularity which is certainly positive but only if it is not used to the prejudice of security.

There are some positive findings too. We found that there are still some fresh new authentication techniques. We can give Password Based Authentication, Zero-knowledge Protocols, Multi-Party Computation or Threshold Authentication as good examples although they are not very commonly used in modern practical systems.

## 2 AAA PROTOCOLS

The most popular protocol analysis is made in this chapter. We focus on a different service support and



Pelka T., Hajny J. and Lambertova P. (2009).
UNIVERSAL AUTHENTICATION FRAMEWORK - Requirements and Phase Design.
In *Proceedings of the International Conference on Security and Cryptography*, pages 57-60
DOI: 10.5220/0002178700570060

on security. We also tried to identify common parts of these protocols as well as different ones to get a starting point for a universal framework design which should support all these solutions.

## 2.1 RADIUS

RADIUS (Remote Access Dial In System) is the first analyzed protocol. It transfers authentication, authorization and configuration data among users. The entities are client, NAS (Network Access Server, typically AP, switch, router...) and authentication server. RADIUS is currently one of the most preferred solutions when we need a protocol for a private network access. It is supported by almost all devices working on an edge of a network.

**Security**

The RADIUS server receives a username and password enciphered by XOR with a MD5 hash. This hash is created by a MD5 function of shared password and random number. This number must be also included to the message so the server can compute the hash too.

**Authentication**

There are many possible authentication methods in the RADIUS protocol. In addition to described methods we can use CHAP, UNIX login, EAP and others. In the case of more complex methods like CHAP there must be a challenge-response phase before the first ACCESS-Request message is sent. Authentication can also run straight between the user and authentication server if we use EAP with tunnelling.

**Accounting**

There is a separate RFC for the RADIUS accounting service. This means that accounting was added to the original protocol by adding of more messages (Accounting-Request and Accounting-Response). These messages collect information needed for billing/logging.

## 2.2 TACACS+

The TACACS+ protocol is another solution. It is quite similar to RADIUS – at least by purpose. The structure is very similar – there is a user who wants to get inside a network and a TACACS+ client with server. The main difference between TACACS+ and RADIUS is the use of the TCP protocol instead of UDP in case of RADIUS and a complete separation of Authentication, Authorization and Accounting.

**Security**

The security is provided by a network packet encryption. TACACS+ uses the MD5 hash and the XOR process which is the same as the RADIUS protocol protection. A shared key is used as secret information. (Rigney, 1997) (Network Sorcery, Inc., 1996)

**Authentication**

The authentication part uses a username and a password by default but other mechanisms are supported too. The protocol is also ready for upcoming techniques.

**Accounting**

A request-response mechanism is used for an accounting service. A request is followed by client data which can be used for billing, audit or monitoring.

## 2.3 Diameter

Diameter is the last interior protocol included to our early framework design. It is a successor of the RADIUS protocol. There is no default compatibility but a compatibility patch exists. The main reason for its creation is a wider network device support. Diameter is especially focused on mobile devices to reflect trends on a market. The most obvious differences from RADIUS are:

- The usage of TCP or SCTP instead of UDP.
- IPSec or TLS is used for an encryption.
- There is a roaming support, error handling, user sessions and direct accounting support.

**Security**

Security is provided by either TLS or IPSec. These protocols are considered to be secure and robust enough.

**Authentication**

Authentication is provided by a new AVP (basic data unit) definition so the flexibility is wide enough. EAP can be used in a standard.

**Accounting**

Accounting is defined by state diagrams similarly as authorization. There are two scenarios – Client Accounting and Server Stateless Accounting (Calhoun, 2003).

## 2.4 Protocol Comparison

We can find many common properties of these protocols (see Table 1, 2 and 3). Many authentication methods are common for more protocols but this does not

necessarily mean that protocols are interchangeable. Different protocols use different ways how to implement these methods.

Table 1: Protocol comparison – RADIUS.

| | **RADIUS** |
|---|---|
| **Protocol** | UDP |
| **Ports** | 1812 – Authentication, Authorization<br>1813 – Accounting |
| **Authentication** | Username/Password, EAP |
| **Authorization** | After valid authentication, authorization data are sent. |
| **Accounting** | Separated - requests are logged |
| **Security** | Shared secret + MD5 |

# 3 UNIVERSAL FRAMEWORK

We provided a brief AAA protocols analysis. We focused on most common solutions for border authentication. It can be seen that there are many solutions and the choice is usually based on the type of a network and user properties. It's also clear that there are many common areas e.g. similar infrastructures or authentication phases. Nevertheless some protocols are much more suitable for some tasks in comparison with other. The main purpose of this chapter is to provide some generalization and create a framework design usable for a wide spectrum of clients with different demands. The design should work as a starting point for further implementation tasks and more complex structures.

## 3.1 AAA Framework Requirements

These criteria are set for the Universal Authentication Framework:

- Security – the system must be secure. This means that it must be built on well established solutions which are regarded to be safe by a technical society.
- Flexibility – the framework must support a wide spectrum of devices from sensors to high end servers. For all of these devices an appropriate AAA service must be chosen. The service must reflect device's capabilities and needs.
- Modularity – the system must lively react on changes in the area of AAA. The introduction of a new technique must be easy.
- Efficiency – the framework must be efficient in a practical deployment so there can't be any unnecessary overhead.

Table 2: Protocol comparison – TACACS+.

| | **TACACS+** |
|---|---|
| **Protocol** | UDP/TCP |
| **Ports** | 49 |
| **Authentication** | Username/Password, Kerberos |
| **Authorization** | Completely separated. |
| **Accounting** | Completely separated. |
| **Security** | Shared secret + MD5 |

Table 3: Protocol comparison – Diameter.

| | **Diameter** |
|---|---|
| **Protocol** | TCP/SCTP |
| **Ports** | 3868 |
| **Authentication** | Username/Password, EAP |
| **Authorization** | After valid authentication, authorization data are sent. |
| **Accounting** | Separated - requests are logged |
| **Security** | IPSec, TLS |

The Universal Authentication Framework (UAF) design was started with these criteria in mind. Current established protocols were chosen as fundamentals because of the security demand. Protocols like RADIUS, Diameter, Kerberos or TACACS+ are considered to be secure enough to work as a core in the first stages of a design process. Another property comes from the demand on efficiency. We decided to add only necessary parts and that's why AAA protocols will not be encapsulated in different data packets but will be used as they are. This will provide both efficiency and compatibility. These protocols will be run as concrete instances of the framework right after the protocol decision phase. That's why we can distinguish 3 main stages of the framework:

1. Handshake – a primary communication between the client and the server. The client specifies a demanded service (all from AAA or just a part) and other parameters used for a protocol decision. The server then chooses appropriate protocol based on this stage and informs the client about protocol parameters (type, IP, port. . . )
2. Service execution – the client has all necessary information so the protocol can be executed. There should be no difference from the normal run of the protocol
3. Record – after the end of the protocol run there is a record phase where data about this run are saved in a server database. These data are later used in a protocol decision.

## 3.2 Handshake

The first stage of the framework is the most critical one. The second and third stage is not difficult to im-

plement (protocols are already developed, a record is trivial) but the first one needs a deeper analysis because it is responsible for an authentication method and connected services choice. We can talk basically about a parametric system which decides about protocol/protocols based on input information. We can model it by a system shown in a Figure 2.

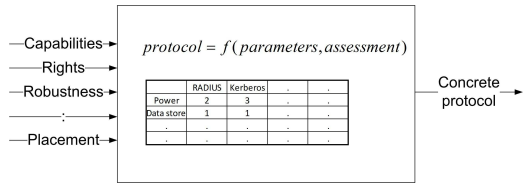


Figure 2: Process of choice.

Information from the client or the server database received during the handshake phase works as an input. The protocol is chosen based on this information and on information from the protocol information table. Information from the handshake can be considered as parameters of the system. The protocol choice process works as follows:

- A new protocol inclusion – It is necessary to create a new record in the protocol information table. The authority must provide information about proof factor (what is used for authentication), security, mobile devices support etc. so the system is later able to do correct decision. This protocol assessment is needed only during the new protocol inclusion.
- Parameters discovery – this is a part of the handshake phase. As all server data are accessible from the database the server needs only data sent by the client.
- Protocol choice – the system analyze the agreement between client demands and server supported protocols. Firstly protocols that does not comply critical demands are rejected. The most suitable protocol is chosen in the second phase. If there is a need for more services than one protocol can support then more protocols are selected. There is no need for more handshakes among these protocols runs.
- Execution – the client gets information about the choice so the service can be provided

We chose only basic protocols for this system by now. The important fact is that there is a possibility to use any authentication method in future. It is also easy to reduce the use of a weak protocol by changes in a protocol information table so it wont be used except inevitable situations.

# 4 CONCLUSIONS

This paper is dealing with the AAA area and is focused mainly on user authentication. We did a current state analysis in the first part. Thanks to a deeper examination we identified a need for a better support of new authentication techniques and easier inclusion of new systems. The Universal Authentication Framework was introduced as a reaction to these findings. Our goal is to solve these problems and provide a solution based on better flexibility and modularity. The dependency on a concrete mechanism is removed. The choice of an actual protocol is made during the handshake stage from extendable set of supported protocols. By this design we get a system where always a most suitable protocol is used for every type of client and where new and better methods can be easily introduced. This also solves the problem of today's networks where varied equipment with very different capabilities and needs meet.

# ACKNOWLEDGEMENTS

Sponsored under the National Program of Research II by the Ministry of Education, Youth and Sports of the Czech Republic in 2C08002 Project - KAAPS Research of Universal and Complex Authentication and Authorization for Permanent and Mobile Computer Networks.

# REFERENCES

Calhoun, P. (2003). Diameter base protocol.

Cao, X. and Li, H. (2006). Secure mobile ip registration scheme with aaa from parings to reduce registration delay. pages 1037–1042.

Hill, J. (2001). An analysis of the radius authentication protocol.

Jiann-Gwo, D. and Cinhg-Song, W. (2007). Secured operation planning on service networks. *ICICIC '07: Second International Conference on Innovative Computing, Informatio and Control*, pages 1–4.

Lee, J.-H. (2007). Architecture for mobile ipv6. pages 1246–1251.

Network Sorcery, Inc. (1996). Diameter.

Rigney, C. (1997). Authentication dial in user service (radius).

Rigney, C. (2000). Radius accounting.