A Universal Frame of Access Control in Computer Networks

Karel Burda

The Faculty of Electrical Engineering and Communication
Brno University of Technology, Brno, Czech Republic

Summary
In the paper, the classification of access control (AC) systems and AC networks is proposed. This classification facilitates the description and security analysis of complex AC systems and networks. The applicability of the proposed terminology and classification is illustrated in the description of a representative range of AC systems and networks. On the basis of this description, we can state that existing solutions of access control use various communication protocols, various message formats, and are intended for various scenarios. The user's access to assets and the cooperation between authorities are complicated by this fact. In the paper, a concept of a universal frame for access control in computer networks is proposed. This frame is based on the idea that all devices of a computer network are equipped with autonomous AC systems (the so-called AC portal), and that these portals can mutually cooperate via a common ACP protocol. The AC portal controls the access of other devices to the assets of a given device or negotiates the access of the applications of the given device to the assets of other devices.

Key words:
Access control, AAA protocol, Authentication protocol, Secure computer network, Authority.

1. Introduction

Computer networks enable their users to use different services. But providers of these services need to control access to the services provided. Most frequently, the objective of this control is the requirement to provide confidentiality of the information provided or the need to enforce payment for the services provided. The control is called access control and ensures that the information or services provided are only available to interested persons to whom access has been permitted by the service provider (the so-called authority). In the case of sizable networks and a large number of users, access control is quite a complicated problem.

The TACACS (Terminal Access Controller Access Control System) network protocol was used to control access in the first packet network (ARPANET) in 1984 [1]. In this protocol, the supplicant connected to the TAC (Terminal Access Controller) access node sent their login and password. The TAC node sent this information to the authentication server (Login Host), which verified it (the so-called authentication). In the case of positive authentication result, the user was linked to the network (the so-called authorization). The need for superior security, performance and reliability has made it necessary to create new protocols for the control of user access to the network. The respective protocols were TACACS+ [2] and RADIUS (Remote Authentication Dial In User Service) [3], [4]. Both these protocols were standardized in 1997 and, in addition to authentication and authorization, they also enabled accounting for the access. In this way, a new class of network protocols came into being, which enabled centralized control and accounting for user access to the network. These protocols are denoted AAA protocols according to the first letters of the functions provided (Authentication, Authorization and Accounting). The latest representative of this protocol class is the Diameter protocol [5] of 2003. This protocol should replace the RADIUS and TACACS+ protocols stepwise.

Simultaneously with the problem of controlling access to networks there also appeared the problem of controlling access to particular information resources and services (i.e. to servers). The same as operators of networks, operators of servers needed to regulate access to the services offered. But in most cases, it was necessary to solve this regulation individually for each particular server and not for more access points as in the case of entire networks. Therefore, only a network authentication protocol needed to be created to control user access because authorization and/or accounting were performed on the given server locally. The Kerberos protocol [6] belongs to the historically first protocols of this type. It was published in 1988. A simpler authentication of users according to the HTTP standard started to be used in web servers in 1996 [7]. But the need for sharing information and services always enforces new solutions (e.g. OpenID [8]).

Both authentication and AAA protocols enjoy considerable boom today. Much attention is being paid to their development and practical deployment [9], [10]. However, the theoretical basis of these protocols, which is the issue of access control, has not attracted any interest. Therefore, this paper is dedicated to expanding and specifying the theory of access control. In the paper, access control is described in general terms and a classification of access control systems and networks is introduced. From this general viewpoint, some of the best known access control systems and networks are characterized. Also, some evolution trends of access control in computer

Manuscript received October 5, 2013
Manuscript revised October 20, 2013

networks are described and, finally, the proposal of a universal frame of access control is described.

2. AC system and its structure

We will refer to data, computer networks, individual computers or network devices and the services provided by them as computer assets or assets for short. A system dedicated to the control of user's access to these assets will be called the access control system (AC system). The owner of assets or an administrator delegated by them will be called the authority. The authority decides about the enlistment of interested persons in a list of authorized users and determines their access rights. The so-called authorization must take place before the enlistment of an interested person in the list of authorized users. Within the scope of authorization, the authority negotiates with the interested person their identity (i.e. their unique name in the list of users), their access rights and their authentication data. The authentication data consist of a proof factor and a verification factor. The proof factor enables the user to prove their identity and the verification factor enables the AC system to verify the identity of the user. Password, private key, fingerprint, etc. are examples of the user's proof factor. Hash of the password, public key, picture of the fingerprint, etc. are examples of the verification factor. In the case of mutual authentication, the factors are negotiated for both directions of authentication. After authorization, the user can ask for access to assets via the AC system.

Physically, the AC system is placed between users and assets (see Fig. 1). This system provides users with access to assets according to their access rights. Data defining access rights of users and their verification factors will be called configuration data. Configuration data are entered into the AC system by the authority. The AC system can collect for the authority some information about the access accomplished (accounting data). This enables accounting for services or performing security audits of user activities.

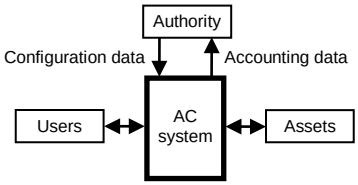

Fig. 1: Placement of the AC system.

Every AC system consists of three basic elements (see Fig. 2), which mutually communicate through a communication system. These elements are:

- gate: an element which enables users access to assets,
- authenticator: an element which verifies the identity of supplicants,
- controller: an element which assures the control of the AC system.

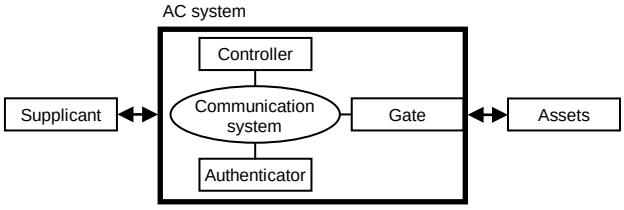

Fig. 2: Structure of the AC system.

Generally, the AC system operates in the following way. First, the user (the so-called supplicant) sends the AC system the request for access to assets. After that, the authentication is performed, which is executed via communication between the supplicant and the authenticator. In the course of this communication, the supplicant must prove that they have at their disposal the proof factor of the respective user. The authenticator verifies this fact using the verification factor, which is obtained from appropriate local or remote database.

The authentication can also be bilateral. In this case, the supplicant and the authenticator exchange their roles in the course of the communication in a defined way. The output of authentication is a message verifying the identity of the supplicant, the so-called authentication result.

The authentication result is forwarded to the controller. In the case of positive authentication result, the controller checks whether all conditions for the permission of access are fulfilled, and establishes the supplicant's rights. As a rule, the controller establishes these rights by looking into the appropriate database or derives them using the rules which are given by the authority. Based on the ascertained rights of the supplicant and, if appropriate, on other context information (e.g. working load of the gates), the controller creates an instruction for the gate. This instruction is a message that permits or rejects access and alternatively describes the supplicant’s access rights and contains other necessary data (e.g. assignment of the IP address to the supplicant). The instruction is forwarded to the gate in a secure way. Based on the instruction for the gate, the controller or appropriate gate generates a notification for the supplicant. This notification is a message for the supplicant that permits or rejects access and alternatively describes the supplicant’s access rights and contains other necessary data (e.g. assignment of the IP address to the supplicant). In the case that it is necessary to perform another authentication between the supplicant and the gate, both the instruction and the notification

contain the necessary authentication factors or the information required for obtaining these factors. The above-described phase of access control will be called access approval or approval for short.

Now, the supplicant has at their disposal the notification while the gate has at its disposal the appropriate instruction. On the basis of information contained in these messages, the two parties enter into communication. In the course of this communication, the gate enables the supplicant to access the assets according to the rights specified in the instruction. If the AC system also registers user activities (the so-called accounting), then the gate sends the controller the information about user access and, if appropriate, also about any other activities of the user (e.g. attempts at unauthorized access). The controller collects and processes this information for a security audit or accounting services. In some AC systems, accounting is not performed by the controller but by a specialized device (the so-called accounting server).

The functioning of the above-described AC system can be illustrated by the schema in Fig. 3. First, the supplicant sends the AC system the request for access to assets. The authenticator verifies the supplicant's identity by the given authentication method (authentication). After this, the controller establishes the supplicant's access rights and formulates them in the form of an instruction for the gate (approval). According to this instruction, the gate enables the supplicant access to assets (access). Optionally, the gate sends information to the controller or accounting server about the access performed by the given supplicant (accounting). In this way, the supplicant's actions are assigned to their identity.

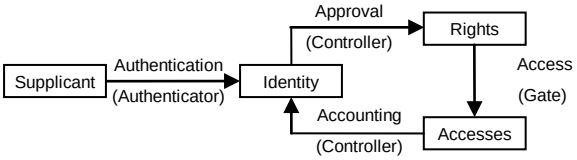

Fig. 3: Functioning of the AC system.

In this paper, we define that the authority is the owner of assets or administrator of the AC system (i.e. the authority is a person and not a device) and the authorization is a one-time act by which the new user, their access rights and necessary authentication data are defined. In the AAA protocols, the controller is usually referred to as the authority and the approval as the authorization [5]. However, this approach introduces confusion in the meaning of basic security terms such as confidentiality or integrity. For example, confidentiality is defined as “ensuring that information is accessible only to those authorized to have access” [11]. If the attacker successfully guesses the password in the process of authentication, the controller issues an appropriate instruction for the gate and the attacker obtains access to assets. If we understand the controller as the authority and the approval as the authorization, then in this case the attacker has been authorized by the authority to have access to confidential information. This is all right according to the wording of the above introduced definition of confidentiality. However, access to confidential information has been granted to a person who does not have permission from the owner of this information. This fact is in sharp contradiction with the intuitive understanding of confidentiality and therefore we reserve the term authority for the person that grants access rights to their assets. For the element of the AC system that controls the AC system we have chosen the term controller.

3. Types of AC systems and AC networks

Access control systems and access control networks are used to control access to computer assets. The access control system (AC system) is a system that is used to control access to computer assets of a single authority. The access control network (AC network) is group of the AC systems of different authorities that mutually cooperate. At first, we will analyze AC systems.

Each element of the AC system can be realized by an individual network device. However, the roles of particular elements are often integrated in practice. Depending on the degree of this integration, we can identify two basic types of AC systems in contemporary computer networks:

- compact AC system,
- distributed AC system.

In the case of the compact AC system (see Fig. 4), all elements of the AC system (i.e. controller, authenticator and gate) are integrated into a single device. This type of AC system will be called the AC portal in the following. An access point according to the IEEE 802.11i standard [12] and the authentication part of the HTTP protocol [13] of a web server are examples of the AC portal. Besides network devices, the AC portal can be found in computers which are not designed for network operation.

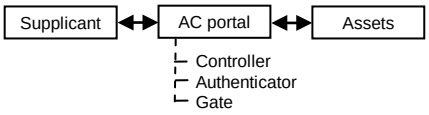

Fig. 4: Compact AC system.

Taken as an example can be a single computer, when the supplicant is trying to obtain access to assets such as processing or information resources of the given computer. The security kernel of the computer controls access to

these assets and therefore this kernel can be practically identified as the AC portal of the given computer.

The distributed AC system consists of two or more network devices. We can classify this type of AC system according to:

- the measure of the centralization,
- the connection of supplicants.

Depending on the measure of the centralization, there are decentralized and centralized distributed AC systems. In the case of the decentralized AC system, the authenticator and controller are different network devices (see Fig. 2). An example of this system is the Kerberos system. In the case of the centralized AC system, the authenticator, controller and, if appropriate, accounting server are integrated into a single network device, which is usually called AAA server (see Fig. 5). Examples of the centralized AC system are most of the systems using the RADIUS, Diameter or TACACS+ protocol. In this case, a single device (AAA server) ensures both the authentication of supplicants and the approval of their access.

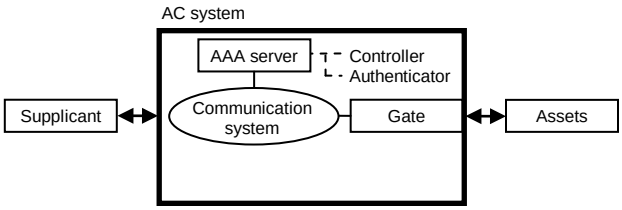

Fig. 5: Centralized AC system.

Depending on the type of the connection of supplicants, we can classify distributed AC systems into systems with:

- direct connection of supplicants,
- indirect connection of supplicants.

In the case of systems with the direct connection of supplicants, the supplicant has access to the communication system which the devices of the AC system use for mutual communication. Thus, the supplicant can communicate with each device of the AC system directly. This organization enables simpler communication and can be used in cases when the communication system is not a protected asset. However, a disadvantage of the direct connection is the fact that supplicants have the possibility of attack the communication in the AC system. For this reason, it is necessary to solve the protection of AC communication. Examples of AC systems with the direct connection of supplicants are systems based on the Kerberos protocol. An AC system with the direct connection of supplicants is illustrated in Fig. 6.

In the case of the indirect connection, the supplicant is connected to some device of the AC system and through this proxy device communicates with other devices of the AC system. This proxy device filters the communication coming from the supplicant and therefore the communication in the AC system is not endangered. Theoretically, the supplicant can be connected to any arbitrary device of the AC system. However, the supplicant eventually obtains access to assets via the gate and therefore the connection via the gate is used in practice. All systems based on AAA protocols (e.g. RADIUS) are an example of the AC system with connection via the gate. The access point of a Wi-Fi network or access switch of a local area network are typical examples of the gate in these AC systems. An AC system with the indirect connection of supplicants is illustrated in Fig. 7.

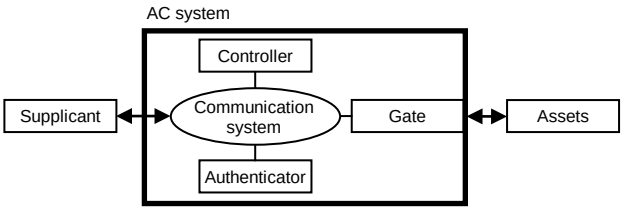

Fig. 6: AC system with the direct connection of supplicants.

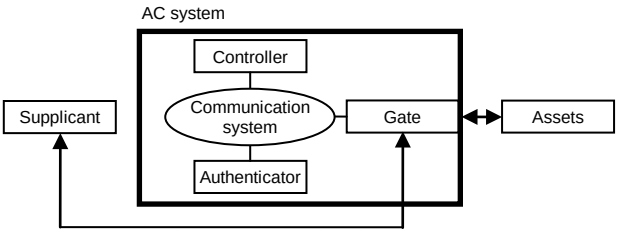

Fig. 7: AC system with the indirect connection of supplicants.

AC systems we have described up to now contain only one controller and therefore will be referred to as one-stage AC systems. We can chain one-stage AC systems into multi-stage AC systems, which contain several hierarchically organized controllers. The hierarchically lowest controller together with its controlled devices (i.e. authenticator and gates) constitutes an AC subsystem. The superior stage can regard this whole AC subsystem as a gate that is controlled by the controller of the given stage. This control is realized by sending instructions to the controller of the AC subsystem. The above-described abstraction of the AC subsystem as a gate can be recursively repeated until the top controller is reached. Fig. 8 illustrates a two-stage AC system.

An example of the two-stage AC system is the access control according to the standard IEEE 802.11i [12]. The hierarchically lowest controller C_1 controls the compact AC subsystem (AC portal), which consists of controller C_1, gate G_1 and authenticator A_1. This whole subsystem

(access point) is understood in the superior stage as a gate G_2. The superior stage is the centralized AC system, which consist of the gate G_2 (and alternatively other gates), the authenticator A_2 and the controller C_2. The authenticator A_2 and the controller C_2 are situated in the AAA server. In contemporary practice, two-stage AC systems are mostly used where the top stage is a centralized AC system and the bottom stage is composed of AC portals. The top stage provides the central management of the access control and the bottom stage provides a higher security level.

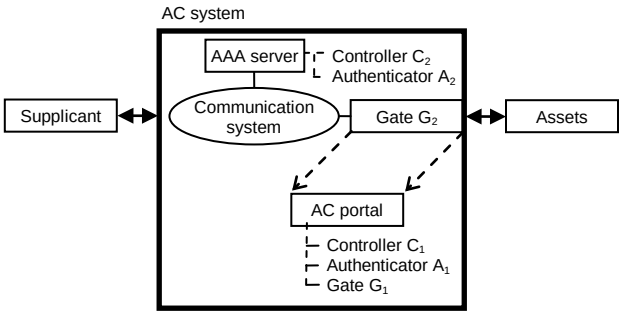

Fig. 8: Two-stage AC system.

We can interconnect the AC systems of different authorities, which gives rise to an AC network. The first possible goal of this interconnection is to enable users of a certain authority access to assets that are protected by AC systems of other authorities. This type of AC network is called the network with cooperating AC systems.

An example of the AC network with three cooperating AC systems is given in Fig. 9.

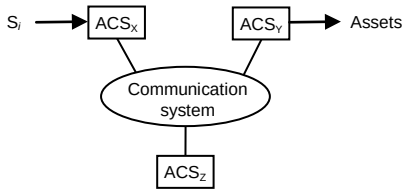

Fig. 9: AC network with three cooperating AC systems.

We have three authorities X, Y and Z. We denote ACS_i the AC system of the authority i, where $i \in \{X, Y, Z\}$. Also, we denote S_X the supplicant who belongs to the set of users administered by the authority X. Analogously, we denote S_Y or S_Z supplicants administered by the other authorities. Let us suppose that supplicant S_i, where $i \in \{X, Y, Z\}$, is connected to the ACS_X and the supplicant's goal is to obtain access to the assets of the authority Y. Then there are three basic variants of the access control. If $S_i = S_X$, then S_X must be authenticated by ACS_X and, subsequently, ACS_X must guarantee ACS_Y the identity of S_X. If $S_i = S_Y$, then S_Y must be authenticated by ACS_Y and, subsequently, ACS_Y must guarantee ACS_X the identity of S_Y. If $S_i = S_Z$, then S_Z must be authenticated by ACS_Z and, subsequently, ACS_Z must guarantee both ACS_X and ACS_Y the identity of S_Z.

A possible solution of access control when $S_i = S_X$ is the following. Let us have an AC network (see Fig. 10) that consists of two cooperating AC systems - the AC system of the authority X (ACS_X) and the AC system of the authority Y (ACS_Y). The authority Y trusts the authority X and therefore the authority Y sets the controller C_Y such that this controller accepts authentication results from the authenticator A_X. After that, the user of ACS_X can obtain access to the assets protected by ACS_Y. Of course, the authentication results must be delivered to the controller C_Y in a secure way.

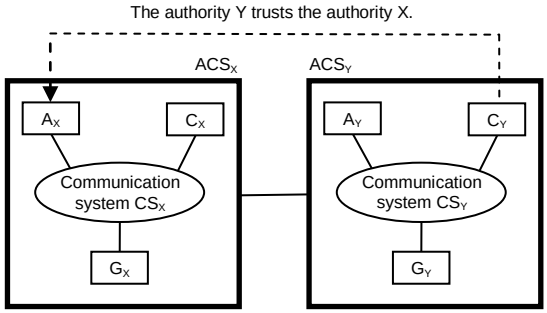

Fig. 10: AC network with two cooperating AC systems.

An example of when $S_i = S_Y$ is the access control according to the RFC 4004 standard [14]. In this standard, the user S_Y of the so-called home network, which is administered by the authority Y, requests access to the home network via the so-called foreign network, which is administered by the authority X. The RFC 4004 standard is explained later in more detail. The case when $S_i = S_Z$ is an extension of the previous case.

The second possible goal for interconnecting AC systems is more effective access control. In this case, some AC systems provide for other AC systems specialized services (e.g. authentication of supplicants). An AC system which provides a service is called the service AC system and a system which uses a service is called the serviced AC system. Therefore, the described type of AC network is called the network with service AC systems.

The service AC system can offer authentication or accounting services. The authentication AC systems offer the authorities of other AC systems the service of authenticating the supplicants. In this case, the serviced AC systems do not have their own authenticator for the authentication of users and accept the authentication results from selected authentication AC systems (see Fig. 11).

An example of this AC network is the AC network with access control according to the OpenID standard [8].

In this case, the so-called OpenID Provider offers the authentication service and its authentication results are accepted by web servers of various authorities (the so-called Relying Parties).

An accounting AC system is an AC system which is dedicated to recording user access to assets of various authorities. Information about user access is sent by the serviced AC systems to the accounting AC system, which records and processes this information. This service enables an effective coordination of billing and settlement between authorities.

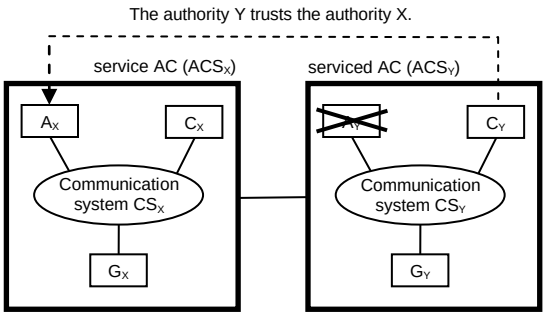

Fig. 11: AC network with the authentication AC system (ACS$_X$).

4. Examples of AC systems and AC networks

Currently, a broad scale of AC systems and networks are in operation. Here, we introduce their representative collection which consists of the standards:

- RFC 2617 (HTTP Authentication),
- IEEE 802.1X,
- IEEE 802.11i,
- RFC 4120 (Kerberos),
- OpenID,
- RFC 4004 (Diameter Mobile IPv4 Application).

The RFC 2617 standard [13] describes controlling the access of a client CL to the web server WS (see Fig. 12).

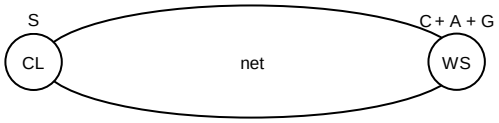

Fig. 12: Access control according to the RFC 2617 standard.

The client and the server are connected by a network and mutually communicate via the HTTP protocol. The supplicant S is the client CL and the assets are the services provided by the server WS. The server is equipped with the AC portal, i.e. it contains an authenticator A, controller C and gate G. After establishing connection, the authenticator executes the supplicant's authentication, the controller establishes the supplicant's rights and the gate enables the supplicant's access to assets according to the rights ascertained. We can see that the AC system described comprises the AC portal of the web server WS and therefore we can characterize this system as a compact AC system.

The IEEE 802.1X standard [15] describes controlling the access of user computers to the local area network (see Fig. 13).

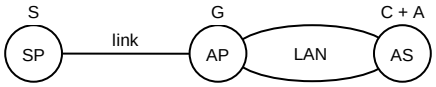

Fig. 13: Access control according to the IEEE 802.1X standard.

The computer SP is connected to the access switch AP by a link. The AP point can communicate with an authentication server AS via a local area network LAN. A suitable link protocol (e.g. according to the IEEE 802.3 standard) is used for communication between SP and AP. A selected AAA protocol (e.g. RADIUS) is used for communication between AP and AS. The supplicant S is the computer SP and the assets are the communication services of the LAN. The authentication server AS performs the functions of both the authenticator A and the controller C. The access switch AP performs the function of the gate G, which also enables the communication between SP and AS. First, the authenticator A executes the authentication of the computer SP. After this, the controller C establishes the supplicant's rights and sends the appropriate instruction to the gate G. Then, the gate G enables or does not enable the supplicant to access the network. We can see that the AC system described consists of more devices (AS and gates) and therefore this system is a distributed AC system. The authenticator and the controller are placed in a single device (authentication server AS) and therefore we can classify the described system more precisely as a centralized AC system. From the viewpoint of the other criteria, we can classify the system as a one-stage AC system with indirect connection of supplicants.

The IEEE 802.11i standard [12] describes controlling the access of a computer to the wireless local area network (see Fig. 14).

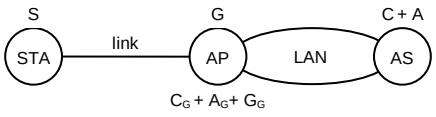

Fig. 14: Access control according to the IEEE 802.11i standard.

The computer STA is connected to the access point AP by a wireless link. The AP can communicate with an authentication server AS via a local area network. The link protocol according to the IEEE 802.11 standard is used for communication between STA and AP. A selected AAA protocol (e.g. RADIUS) is used for communication between AP and AS. The supplicant S is the computer STA and the assets are the communication services provided by the access point AP. In the first phase, the supplicant S communicates with the authenticator A of the authentication server AS. This communication is made possible by the gate G. In the course of this authentication, both parties (i.e. STA and AS) also derive a secret key PMK (Pairwise Master Key). After this, the controller C establishes the supplicant's rights and sends an instruction to the gate G. This instruction must be transmitted in a secure way because it contains the secret key PMK. Now, the computer STA and access point AP know the PMK secret key. From this PMK, they derive the cryptographic keys for authentication and for data encryption between STA and AP.

Now, the second phase of the access control begins. Using the cryptographic keys, the supplicant S and the authenticator A_G execute mutual authentication and an encrypted link is established between S and G. After this, the controller C_G sets the gate G_G into a state when the computer STA can obtain access to communication services provided by the access point AP. The AC system according to the IEEE 802.11i standard is a two-stage AC system. In the hierarchically higher stage, the access point AP performs the function of the gate G and the authentication server AS performs the function of both the controller C and the authenticator A. Thus, in this stage, the AC system is a centralized system with indirect connection of supplicants. In the hierarchically lower stage, the access point AP performs the function of the AC portal.

In the basic version, the RFC 4120 standard alias Kerberos [16] describes controlling the user computer access to the servers of a single authority (see Fig. 15).

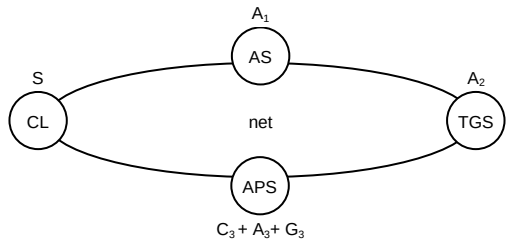

Fig. 15: Access control according to the RFC 4120 standard.

The user computer CL has access to the communication network and therefore can directly communicate with the authentication server AS, requested application server APS and with the administrator server TGS, which administers the application servers of a given authority. The Kerberos protocol is used for the communication between the above devices. The supplicant S is the user computer CL and the assets are the services provided by the server APS. The authentication server AS performs the function of the authenticator A_1, which issues the supplicants with temporary authentication factors for authentication against the server TGS. The administrator server TGS performs the function of the authenticator A_2, which issues the supplicants with one-time authentication factors for authentication against application servers of a given authority. Each APS server contains the access portal $P = C_3+A_3+G_3$. In the first step of the protocol, the supplicant S is authenticated by the authenticator A_1 and obtains a temporary authentication factor, which is usually valid for several hours. For access to some server APS, the supplicant S must be authenticated by the server TGS (i.e. authenticator A_2). In the course of this authentication, the supplicant obtains one-time authentication factors, which are subsequently used for authentication against the requested application server APS. If the authentication between S and A_3 is successful, the controller C_3 establishes the supplicant's rights and sets the gate G_3 in accordance with these rights. We can see that the AC system according to the Kerberos standard consists of more than one device (AS, TGS and APS servers) and therefore we can classify this system as a distributed AC system. Specifically, this system is a decentralized, one-stage AC system with direct connection of supplicants.

Authenticators A_1 and A_2 in the Kerberos system enable separating the administration of users (A_1 in AS) and the administration of servers (A_2 in TGS). This pair also enables building the cooperating AC networks. If some authority X sets their TGS server such that this server accepts authentication factors from the authentication server AS of the authority Y, the users of the AC system of the authority Y can obtain access to the services of APS servers that are administered by the authority X. A necessary condition is that the authority X must appropriately set the controllers C_3.

The OpenID standard [8] describes controlling user access to the web servers of various authorities (see Fig. 16).

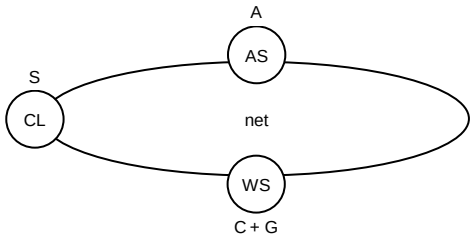

Fig. 16: Access control according to the OpenID standard.

Every user has their identity, which is defined by a specialized authority X. This authority operates their authentication server AS, which knows the verification factors of a given user. The server WS with requested service is managed by the authority Y. The user computer CL, the authentication server AS and the server WS are connected via a network and communicate via the HTTP protocol. The supplicant S is the user computer CL and the assets are the services provided by the server WS. The server WS is equipped with the controller C and gate G. In the first place, the user computer CL logs in to the server WS. If the authentication server AS of the supplicant S is trustworthy for the authority of the server WS, the user computer CL is redirected to the server AS. Subsequently, the user of the computer CL is authenticated by the authenticator A (i.e. server AS). After that, the computer CL is redirected back to the server WS with the authentication result. If the authentication result is positive, the server WS verifies this result by a direct query to the server AS. In the case of positive confirmation, the controller C establishes the supplicant's rights and sets the gate G in accordance with these rights. From this description we can see that the OpenID standard describes an AC network with service AC systems, specifically with authentication AC systems. The server AS is the authentication AC system and the server WS is the served AC system.

The RFC 4004 standard [14] describes controlling the access of a mobile station to a home network via a foreign wireless network (see Fig. 17).

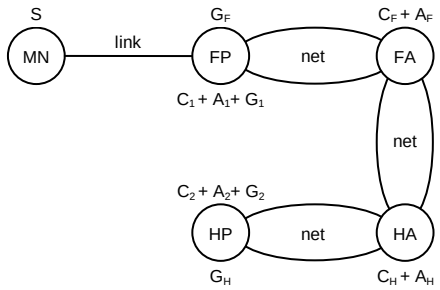

Fig. 17: Access control according to the RFC 4004 standard.

The mobile station MN is connected to the access point FP by a wireless link. The device FP is the access point to the foreign network and is controlled by the server FA, which is an AAA server of the foreign network. The server FA can communicate with the server HA, which is the AAA server of a user's home network. The server HA controls a home agent HP, which enables mobile stations access to its home network. The link protocol according to the IEEE 802.11 standard is used for the communication between MN and FP. The Diameter protocol is used for the communication between FP and FA, FA and HA, and HA and HP. The MIP (Mobile IPv4) protocol is used for the access of the station MN to the agent HP.

The supplicant S is the station MN and the assets are both the communication services of the foreign wireless network and the communication services of the home network. Access control according to the RFC 4004 standard is realized by an AC network that consists of two cooperating two-stage AC systems. The access system of a foreign network consists of the access point FP, which performs the function of the gate G_F, and the server FA, which performs the functions of the controller C_F and authenticator A_F. In the hierarchically lower stage, the gate G_F is the AC portal $P_1 = C_1+A_1+G_1$. The access system of a home network consists of the home agent HP, which performs the function of the gate G_H, and the server HA, which performs the functions of the controller C_H and authenticator A_H. In the hierarchically lower stage, the gate G_H is the AC portal $P_2 = C_2+A_2+G_2$.

The station MN is first authenticated by the authenticator A_H. This authentication communication between MN and HA is enabled by the access point FP and the server FA. If the authentication is successful, the server HA selects several random numbers RN and derives temporary authentication factors from these numbers. These factors will be used for the authentication of the data transmitted between MN and FP, FP and HP, and MN and HP. The server HA also establishes the supplicant's rights and these rights along with the appropriate authentication factors are forwarded to the home agent HP in a secure way. The server HA also forwards the server FA the authentication result, authentication factors for the access point FP and random numbers RN for the station MN. The controller C_F (i.e. FA) establishes the supplicant's rights in the foreign network and this information along with authentication factors for the access point FP and random numbers RN for the station MN are forwarded to the access point FP. The access point FP forwards random numbers RN to the station MN, which derives its temporary authentication factors from these numbers and from its proof factor. Now, the station MN and access points FA and HA have authentication factors at their disposal and the station MN can communicate with the home agent HA via the MIP protocol.

The data between MN and HP (see Fig. 18) are authenticated via message authentication codes (MAC). The authenticators A_1 and A_2 of access points FP and HP verify the authenticity of the data transmitted from MN, i.e. they verify the access rights of MN. Only successfully authenticated packets can pass through gates G_1 and G_2, which are controlled by the controllers C_1 and C_2. In opposite direction of the transmission (i.e. from the home network), FP and MN verify the authenticity of the data transmitted from HP analogously. In this AC system, we can see that the access control is a two-phase process. In

the first phase, the station MN is authenticated and temporary authentication factors are derived in the course of this authentication. In the second phase, the authentication factors obtained are used for continuous authentication of the data being transmitted. In this way, the security of access to assets is increased significantly.

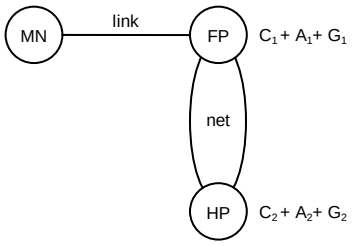

Fig. 18: Access control according to the Mobile IPv4 protocol.

From the above survey of AC systems and networks, we can identify a significant evolution trend, namely increasing the security of access. Increasing the security of access is realized by pushing through the mutual authentication of both parties and pushing through the cryptography protection of the access. Older AC systems are mainly based on a unilateral authentication, when only the supplicant is authenticated (e.g. the original version of the RADIUS protocol). However, in more advanced systems (e.g. IEEE 802.11i, MIP), the bilateral authentication is enforced. In such a case, the supplicant has the guarantee that they really access to the assets of the requested authority.

Let us notice that the access control with bilateral authentication is impossible to describe as an AC system, because what is concerned here is in fact an AC network with two cooperating systems (see Fig. 19). The computer of the supplicant X must be equipped with an internal authenticator, gate and controller, i.e. the supplicant's computer must have its autonomous AC system (ACS_X). This AC system is a compact AC system, i.e. AC portal. The authenticator of ACS_X verifies whether the opposite party is the AC system of the requested authority Y (ACS_Y). According to the result of this authentication, the controller of ACS_X controls the gate of ACS_X and this gate enables the applications running on the supplicant's computer access to the assets of authority Y. The gate of ACS_X can also protect the supplicant's assets against an unauthorized access on the part of ACS_Y. Here, the supplicant X is an authority which decides about access to assets in their computer and about access of applications of their computer to assets of other network devices. AC portals integrated in network devices can significantly increase the security of both the devices and the entire computer networks. Due to the increasing demands on the security, we can expect that implementing AC portals in network devices will be a common issue in the future.

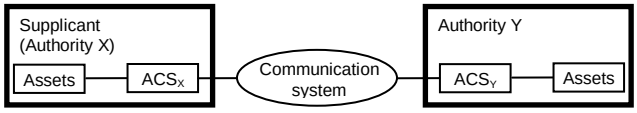

Fig. 19: Access control as an interaction of AC systems of two authorities.

Another way which increases the security of access to the computer assets is implementing the cryptography techniques into the transmission protocol which is used for transmitting data between the supplicant and the gate, i.e. for the access itself. Many modern authentication methods allow both authenticating parties to derive a secret value, which can by used to define cryptography keys. These keys can be used for securing data which are transmitted between the supplicant's computer and the gate of an AC system. In this way, we can assure a continuous authentication of access to assets and not a mere one-time authentication at the beginning of access. Examples of the above solution are the MIP standard and the IEEE 802.11i standard. In the case of the MIP standard, data transmitted between the station MN and home agent HP are continuously authenticated. In the case of the IEEE 802.11i standard, data transmitted between the station STA and the access point AP are continuously authenticated too and, in addition, encrypted.

From the above survey of AC systems and networks, we can see that contemporary AC systems and networks use various communication protocols (e.g. HTTP, Kerberos, RADIUS, IEEE 802.3, etc.), various message formats and different communication scenarios. A negative consequence of this state is the fact that user computers must be capable of handling various protocols for access to assets of various authorities. Another negative fact is that building AC networks is possible only in the case of identical AC systems (e.g. RADIUS). The above negative properties can be eliminated by using a universal protocol for access control. This protocol could enable a unified communication and unified message format for controlling access to assets.

5. Concept of a universal frame for access control

In this chapter, the concept of a universal open frame for access control is described. This frame enables ad-hoc control of access between an arbitrary pair of network devices. Assets can be a service, authentication factor,

communication interface, application, etc. Practically each device of an arbitrary computer network contains certain assets, which it is suitable to protect by some access control method. In this context, an interesting idea would be to implement an autonomous AC system (i.e. AC portal) in each device of the computer network. This portal would control access to the assets of a given device. Simultaneously, the portal would negotiate access to the assets of other network devices for the applications which are running in the given device. Implementing an AC portal in each computer device (i.e. servers, network devices, user computers, authentication devices, etc.) is the essence of the proposed universal frame for controlling access.

According to the proposed concept, individual AC portals mutually communicate via a special protocol for controlling access (Access Control Protocol – ACP). Messages of this protocol enable negotiating the requested assets, negotiating the method of authentication, executing the authentication, approving the access, and accounting. The AC portal of each network device can perform the function of the authenticator, controller or gate, and also forward these messages to other portals. In this way, each network device can perform the function of the authenticator, controller or gate in an arbitrary ad-hoc distributed AC system. An advantage of the frame proposed is a unified and universal solution to controlling access to all assets of all network devices.

The AC portal should be a modular system (see Fig. 20). Then the authority can configure the AC portal of a given device individually according to their requirements and according to the possibilities of the device.

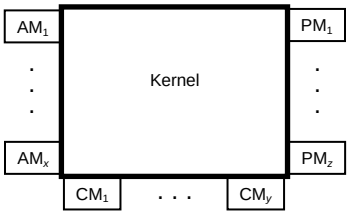

Fig. 20: Modular structure of the AC portal.

The kernel of the AC portal can be complemented with various types of modules. Authentication modules (AM) realize various authentication methods (e.g. module for EAP-TLS authentication). Policy modules (PM) define access policies to the individual assets. The access policy determines conditions necessary for access to a given asset, defines the authentication methods which are allowed for a given asset, specifies the ACP protocol, etc. Messages of the ACP protocol can be transmitted by communication protocols from various layers of the Open Systems Interconnection model, namely from the data link layer up to the application layer. Communication modules (CM) provide an interface between the kernel of the ACP portal and a selected communication protocol.

Examples of the CM module are the TLS, EAPoL and USB modules. The TLS module enables the transmission of ACP messages through the TLS (Transport Layer Security) channel. This channel is suitable for secure communication between AC systems of different authorities. The EAPoL module can enable the transmission of ACP messages through the EAPoL (EAP over LAN) channel. This channel can be used for controlling access of user computers to LAN networks. The USB module can enable the transmission of ACP messages through the USB (Universal Serial Bus) channel. This channel can be used for local communication between computers and authentication tokens.

The above-described universal frame for controlling access provides the possibility of realizing an arbitrary type of the AC system, because each device of a computer network can perform the functions of the authenticator, controller and gate. Fig. 21 illustrates the proposed concept.

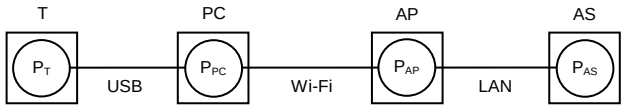

Fig. 21: Illustration of the universal frame of controlling access.

The figure shows the user's authentication device T (token), user computer PC, access point AP and network authentication server AS. All these devices are equipped with an AC portal. We denote these portals P_x, where x = T, PC, AP and AS. For example, if the user wishes to connect their computer PC to LAN network then the computer portal P_{PC} initiates communication with P_{AS} while the P_{AP} transmits the messages of this communication. When the necessary parameters are negotiated, the token portal P_T is involved in the communication too. This portal performs the user's authentication towards authentication server. After obtaining access to the LAN, the process described can be repeated for access to the servers of the given network. In every access, the portal P_{PC} negotiates access parameters (i.e. requested assets and required authentication method) with the portal P_S of the requested server S and the portal P_T authenticates the user. Different assets and different authentication methods can be negotiated for every access, but access protocol is always the same. Other advantages are that the messages of the access protocol can be transferred by different channels (e.g. USB, EAPoL or TLS channel) and that network devices (their AC portals to be precise) participating in the control of the given access

can be different for every access or can function in different roles (e.g. supplicant, authenticator, etc.).

From the example, we can see that the communication for controlling access is unified. Transmitted messages can contain information about assets, information about authentication methods, authentication data, authentication results, instructions for gates, notifications for supplicants, etc. In this way, we can build arbitrary temporary distributed AC systems and networks according to the current requests for access.

In the future, AC portals should become a part of the operating system of a given device. The optimal solution would be to unite the AC portal with the reference monitor of the operating system. The reference monitor controls the access of users and processes to the local data and resources of a given device. Uniting the AC portal with the reference monitor would generally solve the access of users and processes to both local and remote data and resources. AC portals can be implemented in virtual machines too. In this way, we can increase the security of operating systems which are running on these virtual machines.

A combination of the AC portal and the firewall is a promising idea too. In the initial state, the firewall of a given device enables a remote device to communicate with its AC portal only. After negotiating access, the AC portal of the given device sets the firewall such that the packets of the negotiated session are not blocked by the firewall. In the course of mutual authentication, the two AC portals can also negotiate cryptographic keys, which are then forwarded to the appropriate transmission protocol. In this way, the ACP protocol can provide the function of a universal handshake protocol for an arbitrary transmission protocol. In such a case, the ACP protocol performs authentication of parties, negotiates cryptographic keys, and these keys are then used for encryption and authentication of the data being transmitted.

For communication between AC portals, the Access Control Protocol (ACP) was propounded [17]. The ACP protocol is a bilateral protocol. The party requesting access to assets is called the Supplicant and the party providing these assets is called the Provider. A transaction is called one complete run of the ACP protocol, i.e. a sequence of messages between the Supplicant and the Provider which is related to controlling access to requested assets. The format of an ACP message is illustrated in Fig. 22.

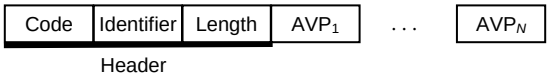

Fig. 22: Message format of the ACP protocol.

The message is composed of a header and *N* attribute-value pairs (AVP), where $N = 0, 1, 2, \ldots$. The basic data unit is the octet (o), i.e. a group of 8 bits. The header of a message consists of the following fields:

- Code (1 o). This field determines the message type (see later).
- Identifier (3 o). This field identifies the transaction in the given channel
- Length (3 o). This field determines the length of the entire message in octets.

The rest of the message consists of zero or more Attribute–Value Pairs. The Attribute–Value Pair (AVP) is a data block in a format as shown in Fig 23.

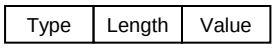

Fig. 23: Format of AVP.

The block AVP consists of the following fields:

- Type (1 o). This field determines the type of AVP, i.e. an attribute (e.g. authentication result, EAP message, etc.).
- Length (1 or 2 o). This field determines the length of the Value field in octets.
- Value (maximum 2^{16}-1 o). This field contains the attribute value. The capacity of this field is sufficient for the transmission of entire EAP messages, cryptography certificates, photos of persons, etc.

Six types of messages are defined in the ACP protocol:

- Start. This message opens a new transaction. The sender of this message is always the Supplicant. The Start message can contain the asset requested (if the Supplicant knows the code of this asset) and the type of authentication (if the Supplicant knows the type of authentication which is required by the Provider for a given asset).
- Finish. This message terminates the transaction and the sender of this message is always the Provider. The Finish message contains the notification for the Supplicant, possibly other data or the asset itself (e.g. digitally signed authentication result).
- Offer. This message is always sent by the Provider and contains the offer of accessible assets or the offer of authentications which the Provider requires for access to a given asset.
- Specification. This message is always sent by the Supplicant as a response to an Offer message. The message contains the Supplicant's choice from the assets or authentication methods offered.

- Request. This message is sent by the Provider and is used for authentication. Authentication is always started by the Provider.
- Response. This message is sent by the Supplicant and is used for authentication.

An elementary transaction of the ACP protocol is illustrated in Table 1. In the first column of the Table, messages sent by the Supplicant are shown. The second column shows the messages sent by the Provider and the third column is dedicated to the notes. Each row of the Table represents one step of the ACP protocol.

Table 1: Elementary transaction of the ACP protocol.

Supplicant	Provider	Notes
Start →		Opening transaction. Opening always by Supplicant.
	Offer ←	Negotiating requested asset. Negotiating can be omitted if Supplicant states the requested asset in Start message or if only a single asset exists.
Specification →		
	Offer ←	Negotiating the type of authentication. Negotiating can be omitted if Supplicant states the appropriate type of authentication in Start message.
Specification →		
	Request ←	Exchanging authentication messages. There can be more Request - Response pairs, depending on the type of authentication.
Response →		
	Finish ←	Provider's notification of approving access and of terminating the transaction.

The ACP transactions can be reduced. The exchange of Offer - Specification messages can be omitted if the Supplicant states the requested asset and appropriate authentication method in the Start message. The exchange of Request - Response messages can be omitted too if the Supplicant and the Provider are the terminal nodes of a secure channel (e.g. TLS channel). The reason is the fact that the authenticity of the opposite party is given by a secured channel. In such a case, the ACP transaction can be reduced to the exchange of only the Start and the Finish messages. This reduction is advantageous for communication between devices of a distributed AC system. For example, the reduced ACP protocol can be used for the communication between the controller and the gate of some AC system. In this case, the Start message contains an instruction for the gate and the Finish message contains a report on the realization of the given instruction. The same approach can be used in the case of accounting.

Only two AC portals (i.e. two devices) participate in one transaction; however, other devices can participate in controlling access too. There are two possibilities how to include more devices. The first possibility is the sequential chaining of more transactions. In this case, the Supplicant obtains some assets in a transaction (e.g. signed authentication result) and uses the obtained assets in the transaction that follows. An example of chaining transactions is the Kerberos protocol, which is a protocol with three chained transactions.

The second possibility of including more devices is inserting a new transaction into the running transaction. In this case, the new transaction must be performed in order to finish the earlier opened transaction. An example is the situation when the Provider opens a new transaction to an external authenticator in order to authenticate the Supplicant (see Fig. 24).

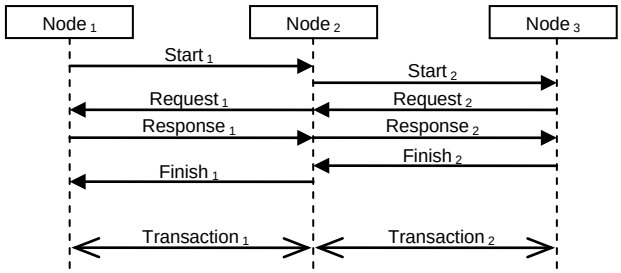

Fig. 24: Example of inserting a transaction.

In this figure, the Supplicant is $Node_1$ and the Provider is $Node_2$. $Node_1$ sends $Node_2$ a message $Start_1$. This message opens $Transaction_1$. The $Start_1$ message contains the requested asset and the appropriate type of authentication and therefore there is no exchange of the Offer and Specification messages. Now, $Node_1$ must be authenticated, but $Node_2$ does not know the verification factor of $Node_1$ and therefore cannot execute this authentication. For this reason, $Node_2$ builds a secure TLS channel to the appropriate authenticator, which is $Node_3$ in this case. In the course of building the TLS channel, $Node_2$ and $Node_3$ are mutually authenticated. $Node_2$ opens the $Transaction_2$ to $Node_3$ in the TLS channel built. In this transaction, the asset is the authentication of $Node_1$, the Supplicant is $Node_2$ and the Provider is $Node_3$. The $Start_2$ message also contains the requested asset and the appropriate type of authentication and therefore the exchange of the Offer and Specification messages does not

take place. Therefore, $Node_3$ immediately opens authentication by sending the $Request_2$ message. $Node_2$ extracts appropriate AVPs from this message and sends them in the $Request_1$ message, which is a $Transaction_1$ message. $Node_1$ calculates an authentication reply and sends this reply to $Node_2$ in the $Response_1$ message. $Node_2$ extracts appropriate AVPs from this message and sends them in the $Response_2$ message, which is a $Transaction_2$ message. $Node_3$ executes authentication calculations and sends the result of authentication in the $Finish_2$ message. At the same time, this message terminates $Transaction_2$. On the basis of the authentication result, $Node_2$ decides about the access to the requested asset and this decision is sent to $Node_1$ in the $Finish_1$ message.

The above-described insertion of ACP transactions is suitable for AC systems with indirect connection of supplicants. The chaining of ACP transactions is suitable for AC systems with direct connection of supplicants. An arbitrarily complex access control can be described as a diagram of bilateral transactions, which are chained or inserted in a certain way. This approach enables easier implementation and more transparent security analysis of complex schemes of access control.

An ad-hoc communication network is built for the communication between nodes. This network consists of nodes which are necessary for the particular case of access control. The nodes are interconnected by secure channels, which are typically TLS channels or physically secured links. These channels can be either the permanent channels (typically between nodes of an AC system) or the temporary channels (typically between nodes of different AC systems).

The specific arrangement of transactions for the control of access to assets of a given device is configured by the authority. The appropriate PM module contains these configuration data. Here, the authority can individually set the control of access to the given asset. In the PM module, the authority also sets the network addresses of accepted authenticators, the network address of the superior controller, certificates of public keys, etc. There are specialized AVPs (e.g. data container encrypted by AES cipher) for securing the ACP protocol. The particular way of message exchange in the transaction and securing these messages are determined by authority.

6. Conclusion

The paper specifies and extends the theory of access control. In the paper, the terminology (terms such as gate, controller, authority, authorization) is specified and new terms (AC system, AC subsystem and AC network) are introduced. In addition, the classification of AC systems and AC networks is proposed in this paper. This classification facilitates the description and security analysis of complex AC systems and networks.

The applicability of the proposed terminology and classification is illustrated in the description of a representative range of AC systems and networks. On the basis of this description, we can state that existing solutions of access control (e.g. RADIUS, Diameter, Kerberos, etc.) use various communication protocols, various message formats, and are intended for various scenarios. The user's access to assets and the cooperation between authorities are complicated by this fact.

In the paper, a concept of a universal frame for access control in computer networks is proposed. This frame is based on the idea that all devices of a computer network (servers, user computers, authentication devices, etc.) are equipped with autonomous AC portals, and that these portals can mutually cooperate via a common ACP protocol. The AC portal controls the access of other devices to the assets of a given device and negotiates the access of the applications of the given device to the assets of other devices. Each AC portal is equipped with an authenticator, controller and gate and therefore, each network device can perform an arbitrary function in some AC system. The idea described in this paper makes it possible to build a distributed ad-hoc AC system for an arbitrary situation from the AC portals of participating devices.

A possible bilateral ACP protocol has been described for communication between AC portals. Messages of this protocol enable negotiating the requested assets, negotiating the method of authentication, executing the authentication, approving the access, and accounting. An arbitrarily complex access control can be implemented by a combination of ACP protocol transactions, which are chained or inserted in a certain way. Chaining and inserting transactions also enables a modular and systematic secure analysis of the proposed AC systems. From the viewpoint of syntax, the ACP protocol is an open protocol, which can be expanded in the future.

Messages of the ACP protocol can be transmitted via various transmission protocols and interfaces (e.g. TLS, EAPoL, and USB). The AC portal has a modular structure and therefore the authority can configure portals precisely according to their needs and according to the possibilities of network devices. The authority can set various authentication methods and various conditions for the access to each asset. The AC portal can be integrated with the reference monitor of the operating system, which offers the possibility of unifying the control of access to the local and remote assets. The AC portal can also control the firewall and in this way, only sessions when the opposite party has been authenticated are allowed.

A disadvantage of the proposed frame is the fact that the implementation of this frame demands relatively

significant changes in existing solutions because AC portals should be implemented in the secure kernel of operating systems. This process will be relatively slow and complex, in particular for devices with restricted computational power (e.g. authentication tokens). On the other hand, the implementation of AC portals can significantly increase overall security of computers and computer networks.

References

[1] Dennet S, Feinler EJ, Perillo F.: Arpanet Information Brochure. Defense Communication Agency. Menlo Park, 1985.
[2] Carrel D, Grant L: The TACACS+ Protocol. IETF, Fremont, 1997.
[3] Rigney C, Willens S, Rubens A, Simpson W: Remote Authentication Dial In User Service (RADIUS). IETF, Fremont, 2000.
[4] Rigney C: RADIUS Accounting. IETF, Fremont, 2000.
[5] Calhoun P, Loughney J, Guttman E, Zorn G, Arkko J: Diameter Base Protocol. IETF, Fremont, 2003.
[6] Miller SP, Neuman BC, Schiller JI, Saltzer JH: Kerberos Authentication and Authorization System. M.I.T. Project Athena, Cambridge, 1988.
[7] Berners-Lee T, Fielding R, Frystyk H: Hypertext Transfer Protocol -- HTTP/1.0. IETF, Fremont, 1996.
[8] OpenID. OpenID Authentication 2.0. OpenID Foundation, San Ramon, 2007.
[9] Nakhjiri M, Nakhjiri M: AAA and network security for mobile access. John Wiley & Sons, Chichester, 2005.
[10] Lopez J, Oppliger R, Pernul G: Authentication and authorization infrastructures (AAIs): a comparative survey. Computers & Security 2004, 23, 578-590.
[11] ISO/IEC 17799:2005. Information technology - Security techniques - Code of practice for information security management. ISO, Geneva, 2005.
[12] IEEE 802.11i. Medium Access Control (MAC) Security Enhancements. IEEE, New York, 2004.
[13] Franks J, Hallam-Baker P, Hostetler J, Lawrence S, Leach P, Luotonen A, Stewart L: HTTP Authentication: Basic and Digest Access Authentication. IETF, Fremont, 1999.
[14] Calhoun P, Johansson T, Perkins C, Hiller T, McCann P: Diameter Mobile IPv4 Application. IETF, Fremont, 2005.
[15] IEEE 802.11X. Port-Based Network Access Control. IEEE, New York, 2004.
[16] Neuman C, Yu T, Hartman S, Raeburn K: The Kerberos Network Authentication Service (V5). IETF, Fremont, 2005.
[17] Burda K, Strasil I, Pelka T, Stancik P: Access Control Protocol (ACP). [Draft]. IETF, Fremont, 2011. URL: http://tools.ietf.org/html/draft-kaaps-acp-01

Karel Burda received the M.S. and PhD. degrees in Electrical Engineering from the Liptovsky Mikulas Military Academy in 1981 and 1988, respectively. During 1988-2004, he was a lecturer in two military academies. At present, he works at Brno University of Technology. His current research interests include the security of information systems and cryptology.