The Model and Control Methods of Access to Information and Technology Resources of Automated Control Systems in Water Supply Industry

M Yu Rytov[1], S A Spichyack[1], V P Fedorov[2] and D I Petreshin[3]

[1] Department of Information Security Systems, Bryansk State Technical University, Bryansk, Russia
[2] Department of Mechanical Engineering and Technology, Bryansk State Technical University, Bryansk, Russia
[3] Academic and Scientific Technological Institute, Bryansk State Technical University, Bryansk, Russia

E-mail: rmy@tu-bryansk.ru

Abstract. The paper describes a formalized control model of access to information and technological resources of automated control systems at water supply enterprises. The given model considers the availability of various communication links with information systems and technological equipment. There are also studied control methods of access to information and technological resources of automated control systems at water supply enterprises. On the basis of the formalized control model and appropriate methods there was developed a software-hardware complex for rapid access to information and technological resources of automated control systems, which contains an administrator's automated workplace and ultimate users.

1. Introduction

The object of research is the control procedure of access to information and technological resources in the automatic control system of a water supply enterprise. Modern water supply enterprises belong to critical objects of housing and communal services and have a great number of technological objects and information resources. These resources in practice are integrated under the control of an automated system including such components as ERP-systems, DBMS (database management system), ACS technological equipment (ACS - automatic control system), communication systems with mobile and stationary objects and their positioning etc.

Object control in the system is directive and centralized. The automatic control system of a water supply enterprise has a lot of various communications paths: a local-area network (LAN), half-duplex radio communication with radio modems, GSM channel communication, analog telecommunication and others.

The control environment is defined as trustful. The technological information circulating in the system is not confidential, but there is a need of ensuring its availability, reliability (authenticity) and access isolation within the trusted environment.

The urgency of the modelling problem is caused by occasional and systematic failures of communication links. There is a reduction of personnel and a systematic shortage of shifts at

enterprises. As a result there is a need to ensure a quick cross access to technological and information resources in case of difficult and emergency situations.

So we carried out the comparative analysis of describing models of access isolation in different sources. We also consider classical models of access isolation in computer systems: discretionary, mandatory, role-based access. The model of cross access demarcation is also studied [1].

The research objective is developing the model and control methods of access to information and technological resources of an automated control system at water supply enterprises.

Within this objective, the following tasks are solved:

- development of a mathematical model of the research object, including its features;
- development of methods to control the access and ensure access reliability:
  - deposition and preliminary distribution of authenticators,
  - ensuring quick cross access in emergency,
  - control of the period of access authority by means of authenticator evolution;
- development of the automated control subsystem of access to information and technological resources.

2. The formalized control model of access to information and technological resources of automated control systems at water supply enterprises.

Taking into account the peculiarities of this process and the previous works in the field [2,3], we have developed the formalized control model of reliable access to information and technological resources of the automatic control system of a water supply enterprise.

Nominally, it is defined as follows:

$$M = \langle U, T, S, P, R, Z, G, F \rangle, \tag{1}$$

where $U = \{u_1, u_2, ..., u_{uc}\}$ is a set of access subjects (users/subscribers), if *uc* is a number of access subjects. Each subject has a set of unique identifiers (within the user group). $I = \{i_1, i_2, ..., i_{ik}\}$ is a set of identifiers, if *ik* is an amount of identifiers. Identifiers serve for unambiguous recognition of subjects among all set members *U*. Also, each subject has a set of authenticators from set *A*, by means of which it is possible to confirm the personality and the rights of the subject. Therefore, $A = \{a_1, a_2, ..., a_{ak}\}$ is a set of authenticators, if *ak* is an amount of authenticators. The following functions were introduced: $user: I \to U$, $id: A \to I$. They join the set of basic functions of system *F*, i.e., $user, id \subset F$.

$T = \{t_1, t_2, ..., t_{tc}\}$ is a set of information and technological resources (objects), if *tc* is an amount of resources. Each resource has one or more set members of communication links $C = \{c_1, c_2, ..., c_{ck}\}$, if *ck* is a number of channels, with the appropriate sets of safety protocols $K = \{k_1, k_2, ..., k_{kc}\}$, if *kc* is a number of protocols which are also unambiguously connected with the current authenticator of $a_j \in A$. We introduced the following ratio:

$$resourses = \{(t_i, k_j, a_j) | (i \le tc) \wedge (c_k \in C)\}. \tag{2}$$

$S = \{s_1, s_2, ..., s_{sc}\}$ is a session identifier, if *sc* is a number of such session identifiers. The element of this set is created at the first appeal of the subject to the object, when the subject passes identification and authentication. The identifier and an authenticator are stored in the session and do not demand repeated input at the appeal to resources. The following functions are introduced: $sid: S \to I$, $suser: S \to U$, $sauth: S \to A$. They join the set of basic functions of system *F*, i.e., $\{suser, sid, sauth\} \subset F$.

$P = \{p_1, p_2, ..., p_{pc}\}$ is a set of access rights, if pc is an amount of access rights. This set contains all possible access rights to resources. The following relations are introduced: $UP = U \times P$ is a relation setting correlation between subjects and access rights, and $PH = P \times P$ is a relation of a partial order (hierarchy) in the set of access rights indicated by "$\succeq$". The following functions are introduced: $permission: U \to 2^P$ is a function correlating subject *ui* with a set of access rights

$permission:(u_i)\subseteq\{p\,|\,(\exists p_0\succeq p)\wedge((u_i,p_0)\in UP)\}$. They join the set of basic functions of system F, i.e., $permission:(u_i)\subseteq\{p\,|\,(\exists p_0\succeq p)\wedge((u_i,p_0)\in UP)\}$.

$R=\{r_1,r_2,r_3,r_4,r_5\}$ is a set of roles within system: r_1 - "unauthorized user", r_2 - "authorized user", r_3 - " resource administrator ", r_4 - " user group administrator" and r_5 - "network administrator". The following relations are introduced: $UR=U\times R$ is a relation correlating subjects and roles, $RP=R\times P$ is a relation correlating roles and access rights, $RH\in R\times R$ is a relation of a partial order (hierarchy) in the set of roles indicated by "$\succeq$". The following function is introduced: $role:S\to R$ is a function correlating s_i session, one of the roles acceptable in *R*.

$Z=\{z_1,z_2,...,z_{zc}\}$ is a set of access servers, if *zc* is an amount of access servers included into the network. One access server can serve several groups, subscribers, resources, i.e. $z_i=\langle u_i,t_j,g_k\in G\rangle$.

$G=\{g_1,g_2,...,g_{gc}\}$ is a set of user groups, if *gc* is an amount of user groups. Each user u_j is included into user group g_i, i.e., $u_i\subset g_i$ for $j\in\{1,...,uc\}$ and $i\in\{1,...,gc\}$. The g_i group also includes the following relation:

$serv:Z\to G;autorization:t_i\times\{permission(u_k)\,|\,u_k\in U\}\times$

$\times U\to\{ok,access\ denied\}$.

They join the set of basic functions of system *F*: $\{serv,autorization\}\subset F$.

$F=\{user,id,suser,sid,sauth,permission,serv,autorization,role\}$ is a set of the system basic functions.

We defined the following rules:

- A rule of interacting users and information resources of various workgroup under the system control. Each information resource correlates with a set of couples like $\langle g,privacy\rangle$. In this case, a user has access to a resource only if the resource belongs to the user's domain, and the level of his access privilege is more or equals the level of resource privileges. So, user *u* has an access to resource *t*, if:

$$\exists\langle g,privacy\rangle\in D_r(t):g\in D_p(u)\wedge privacy\geq access(u),$$

where D_r is an operator which receives a set of couples defining a resource (a characteristic set); D_p is an operator which receives a set of domains (domain hierarchy), to which the user belongs; *access* is a function of the user admission level.

- A rule of providing a quick cross access to technological resources. Each technological resource correlates with a set of couples $\langle a,c\rangle$ and the access is provided if the user is authorized for this session in the communication link with the resource by correlation *resourses* :

$$\exists\langle a,c\rangle\in D_c(t):a\in A,c\in C:a\in sauth(s)\wedge resourses(t,k,a,c)$$

where D_c is an operator which receives a set of couples defining the used channel and the protocol of communication with the resource (a characteristic set).

This model takes into account that there are different communication links with information systems and technological equipment. Besides, it was determined that for increasing control flexibility the model allows introduction of additional restrictions on the combinations of components, for example: restrictions of the subject's access rights on the quantity of sessions or on time and so on.

3. Control methods of access to information and technological resources of automated control systems at water supply enterprises.

The group of methods provides combined use of the control model of access, schemes of preliminary distribution of authenticators, schemes of secret share for development of a temporary access authenticator and an algorithm of authenticator evolution.

In the trusted communication environment, it is recommended to use a unique identifier for communication between each couple of subscribers. This results in a need for a network of *n* subscribers to generate and store *n* (*n* - 1)/2 authenticators. And each of *n* subscribers should store *n* - 1 authenticator.

Application of schemes of preliminary distribution of authenticators allows (Blom, KDP and others) to reduce the number of authenticators generated and stored in the automated control system.

Let us consider Blom's scheme as a basic scheme of preliminary distribution of authenticators [5]. In this scheme, finite field F fixes n different nontrivial elements $r_1, \ldots, r_n \in F$ which are attributed as identifiers to network subscribers. Then a polynomial is chosen over finite field F $2m$, $1 \le m < n$, like

$$f(x,y)=\sum_{i=0}^{m}\sum_{j=0}^{m}a_{ij}x^i y^j, \tag{3}$$

which factors a_{ij} form an invertible square matrix of authenticators symmetric to main diagonal $\Lambda=(a_{ij})_{m\times m}$ over finite field F.

Matrix Λ is confidential and is deposited on the authentication server. Each subscriber A receives set $\left(a_0^{(A)}, a_1^{(A)}, ..., a_m^{(A)}\right)$ consisting of polynomial factors as a universal authenticator:

$$g_A(x)=f(x,r_A)=a_0^{(A)}+a_1^{(A)}x+...+a_m^{(A)}x^m. \tag{4}$$

Then, a unique authenticator of k_{AB} is used for communication between each couple of subscribers A and B:

$$k_{AB}=k_{BA}=f(r_A,r_B)=g_A(r_B)=g_B(r_A), \tag{5}$$

which finally allows to store m authenticators instead of n - 1.

In Blom's classical scheme, identifiers are in open access. When using a combined (matrix and role) access, we determine correlation in the access matrix between the subscriber's rights seeking access and an r_B identifier of the requested information resource or the requested subscriber.

Technological resources often have a fixed access authenticator. Besides, when arranging a cross access, the subscriber's authority can be limited on time or number of sessions. Denial of service by the authentic (protected) communication link is also possible. For emergency access, it is offered to use a combination of the scheme of preliminary authenticators' distribution and the scheme of the full secret share [4]. Let us assume that it is necessary to provide an access to technological resource U having a fixed k_U authenticator. In this case, the authentication server generates accidental bit vector b of length m:

$$b = (b0, b1, \ldots, bm)2. \tag{6}$$

Also temporary authenticator r' is calculated (over GF_2 field.):

$$r'=k_U+\sum_{i=0}^{m}b_i a_i^{(A)}\cdot \tag{7}$$

Temporary authenticator r', calculated in this way, and accidental vector b are transferred to the subscriber by the open reserve channel. Having received them the subscriber can retrieve the k_U authenticator (over the GF_2 field.):

$$k_U=r'+\sum_{i=0}^{m}b_i a_i^{(A)} \tag{8}$$

To increase security, it is possible to use function of hashing of $H(x)$ in addition to summing of authenticators:

$$r'=k_U+H\left(\sum_{i=0}^{m}b_i a_i^{(A)}\right). \tag{9}$$

Carrying out a similar combination is also possible on the basis of scheme KDP [6] founded on intersection of sets. For $n > 2$ subscribers and sets of authenticators of A, $|A| = q$, direct numbering of authenticators 1, 2, ..q is defined. We choose some family $\{S_1, \ldots, S_n\}$ of set subcollections $\{1, 2, \ldots, q\}$, which is Shperner's family in which one subcollection does not contain another. In the original KDP scheme, family $\{S_1, \ldots, S_n\}$ represents an unclassified table with numbers of authenticators from set a_{ik}, $k \in S_i$, previously transferred to each subscriber by the secure channel. When using a combined (matrix and role) access, we determine correlation in the access matrix between the subscriber's rights seeking access and S_i element of the requested information resource or the requested subscriber.

To develop a common communication authenticator between subscribers of A and B, we use intersection $S_A \cap S_B$. For example:

$$k_{AB} = k_{BA} = \sum_{i=1}^{|S_A \cap S_B|} a_i \ \text{over}\, GF_2. \tag{10}$$

If there is a need to provide an access to technological resource U having a fixed k_U authenticator, the authentication server generates accidental bit vector b of length $m = |S_A|$, as it was in the previous case:

$$\text{b} = (\text{b0}, \text{b1}, \ldots, \text{bm})2. \tag{11}$$

Also temporary authenticator r' is calculated:

$$r' = k_U + H\left(\sum_{i=0}^{m} b_i a_i\right). \tag{12}$$

Temporary authenticator r' calculated in this way and accidental vector b are transferred to the subscriber by the open reserve channel. Having received them, the subscriber can retrieve the k_U authenticator as in the example above.

The drawback of the methods described above is that the k_U authenticator received by subscriber A is constant. To stop temporary emergency access rights of subscriber A to resource U, we offer to use evolution of technology resource authenticators.

We consider the following methods of authenticators' evolution: Lamport's protocol of one-time authentication [7]; dynamic authenticator change in a gamming mode (CTR); combination of two previous methods.

When using Lamport's protocol for each technology resource U having a fixed k_U authenticator, we determine action duration L_U of basic authenticator k_U and estimated frequency of replacement L_i of temporary authenticators k_{Ui}. Then, a required amount of periods $t = L_U/L_i$ is calculated. On the basic step of the protocol, a one-way function of hashing $H(x)$ is used. Temporary authenticator k_{Ui} is defined for the current i - period of action:

$$k_{Ui} = \underbrace{H\left(H\left(\ldots\left(k_U\right)\ldots\right)\right)}_{t-i \text{ times}} = H^{t-i}\left(k_U\right) \tag{13}$$

Thus to provide temporary access rights to subscriber A, the authentication server transmits by an open communication link: accidental binary vector b, the action period of authenticator L_i, period number i, the amount of periods t and temporary authenticator r' are calculated as:

$$r' = \underbrace{H^{t-i}\left(k_U\right)}_{k_{Ui}} + H\left(\sum_{i=0}^{m} b_i a_i^{(A)}\right). \tag{14}$$

Having received them, the subscriber can retrieve the k_{Ui} authenticator operating during period T_i:

$$k_{Ui} = r' + H\left(\sum_{i=0}^{m} b_i a_i^{(A)}\right). \tag{15}$$

The shortcomings of this method are the limited period of the authenticator k_U action, and also an increase of computing loading at the high intensity of information exchange.

When using the gamming mode, authenticator k_U dynamically changes within some period L_i by means of enciphering in the gamming mode. Authenticator k_{Ui} is the recurrent fraction of block gamma:

$$\text{kUi} = \text{Ts}\ (\text{eK}(\text{CTRi})), \tag{16}$$

where $CTR_1 = IV$ is an initiating vector (synchronous packet),
$CTR_i = inc(CTR_{i-1})$ is a register value,
e_K is an encryption block algorithm on secret key K,
T_s - procedure of taking seniors s bits.

In this case, authenticator k_U can act both as key *K* and as synchronous packet *IV*.

Two methods described above can be combined as follows. By means of Lamport's protocol temporary administrator of a technological resource, an authenticator, used as a *K* key, is given, and the administrator in its turn can transfer users temporary authenticators generated in the CTR mode, using the simplified way of generation *r'*:

$$r' = k_{Ui} \oplus H(k_{AB}) \oplus b \tag{17}$$

where k_{AB} is a common communication authenticator between the user and the administrator.

4. Conclusion

The given model considers the availability of different communication links with information systems and technological equipment. Besides, it has been determined that in order to increase control flexibility, the model allows introduction of additional restrictions on combinations of components, for example: restrictions on the subject's access rights by session amounts or on time and so on.

On the basis of the formalized model and methods of access control, there has been developed a hardware-software complex of rapid access to information and technological resources of automated control systems for water supply enterprises. This complex consists of the administrator's automated workplace and ultimate users.

The program components of the complex implement are:

- the scheme of authenticators' preliminary distribution (Blom's scheme, KDP), in combination with access policies;
- support of authenticators' evolution on the basis of Lamport's protocol or the Counter (CTR) mode;
- generation and transfer of temporary access authenticators using the combination of the scheme of authenticators' preliminary distribution and schemes of the full secret share.

The program part of the complex is implemented with the use of high-level libraries of the PKCS#11standard [8] and the Rutoken CSP crypto service provider, which is the main to provide authentication and integrity (CMAC message authentication code development and other cryptographic transformation). The subsystem is multiplatform and it imposes low system requirements. This provides connectivity with the hardware of technological equipment. The complex hardware is represented by cryptographic identifiers Rutoken ECP Flash and technology equipment controllers.

References

[1] Demidov A V, Ofitserov A I and Afonin S I 2010 *Information technologies in science, education and production* **5** 94-101
[2] Eryomenko V T, Mishin D S, Paramokhina T M, Eryomenko A V and Eryomenko S V 2014 *Information systems and technologies* **3** 51-58
[3] Eremenko V T and Paramokhin V M 2015 *Information systems and technologies* **2(88)** 131-137
[4] Rytov M Yu, Shpichak S A, Pavlinova I V and Pavlinova E I 2014 *Cryptographic providing information protection* 220
[5] Blom R 1983 *Nonpublic key distribution, Advances in Cryptology, Proceeding of EUROCRYPT '82 Plenum New York* 231-236
[6] Dyer M, Fenner T, Frieze A and Thomason A 1995 *On key storage in secure network, J Cryptology* **8** 189-200
[7] Lamport L 1978 *Communications of the ACM* **21(7)** 558-565
[8] PKCS #11 Base Functionality v2.30: Cryptoki - Draft 4, RSA Laboratories 2009