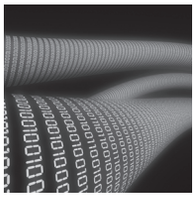

Archives of
Transport System Telematics

Volume 2

Issue 2

May 2009

The safe access control into ITS distributed databases

M. SVÍTEK
Faculty of Transportation Sciences, Czech Technical University in Prague, Konviktská 20, 110 00 Prague 1, Czech Republic
EMAIL: svitek@fd.cvut.cz

ABSTRACT
Paper presents new method how to share and process the sensitive data distributed in different databases. It is typical for ITS area that data elements are stored and managed by different public/private organizations located on different places. On the other hand a lot of telematics applications are based on the connections and further processing of shared data elements. This fact yields into requirements for new dynamical electronic identifiers that protect communication channel against sensitive information connection. We present the basic concept of application of dynamical identifiers together with illustrative example applicable for e-Government part of ITS.

KEYWORDS: electronic identification in ITS, safe access control, dynamic identifiers

1. Introduction

We identified the request for better solution of access control into sensitive data elements [1, 2] that are spatially distributed in different organizations. We can assume that data elements only from one database can not carry sensitive information but the problem of "big brother" appears in case two or more data elements from different databases are connected.

As an example, we can use two different databases – in one database are stored data elements about car owners, and in second one the data about cars. In both databases we can use generated "artificial" identifiers pointed out on different data elements. Both databases can be separately used for statistics of car owners' age in different regions, cities, time series of luxury car penetration, etc. But only knowledge of rule how to generate identifiers in both databases can provide us with information how to connect both databases and only this knowledge yields into problem that e.g. somebody knows that I am the owner of this type of luxury car.

We try to overcome this problem and we present the method how to protect the data connection in both databases and also in communication channel. Our original solution combines the fix- and dynamical identifiers where dynamical identifiers are time dependent. In chapter 2 we introduce the basic principle of safe access control system into distributed databases. Chapter 3 covers illustrative example from ITS area in e-Government and chapter 4 concludes paper.

2. Basic principles of safe access control system

Basic principle of safe access control system into distributed databases is given on fig.1. We can define following main parts:

- A – spatially distributed databases (in fig.1 there are two databases with indexes j, k)
- B – safe access control area with fix- and dynamical identification modules
- C – ITS applications using the data from spatially distributed databases (in fig.1 there two application x and y)

- D – dynamical and communication system that is responsible for safe data transmission between spatially distributed databases and ITS applications.

The first principle, necessary for data from different databases connection, yields into fix data identification provided in subsystem (3). This approach can also be named as "unified databases synchronization" because we start with generation of unique fix identifier (3.1) for all connected data elements stored in different databases.

The same identifier for all databases is not safe and databases connection is in this case very easy. It is the reason why we extended unique fix identifier (3.1) into different fix identifiers assigned to different databases. This principle enables us to store data elements assigned into same event in different databases with different identifiers. It means that only authorized person who knows unique fix identifier (3.1) and algorithm how to generate different fix identifiers (3.2) can connect data elements from two or more databases. The generation function of fix identifiers (3.2) must be one-directional – it means, that it is not possible to mathematically generate unique fix identifier (3.1) based only on knowledge of all fix identifiers (3.2).

The set of fix identifiers assigned to different databases can protect information connection but there is serious problem – communication message monitoring. If somebody will listen to on transmitted messages through information and communication system (D) sooner or later he is able to reconstruct "static table" of different databases' identifiers that enable him the connection of sensitive data elements.

We add into subsystem (B) also module for dynamical identification that generate dynamical identifiers (4.1) that are time dependent. It means that each data transaction through communication channel (D) is realized with help of different identifiers that are valid only in time of transaction. No message monitoring in channel (D) can break this safety principle because we cannot reconstruct "dynamic table" of different databases' identifiers.

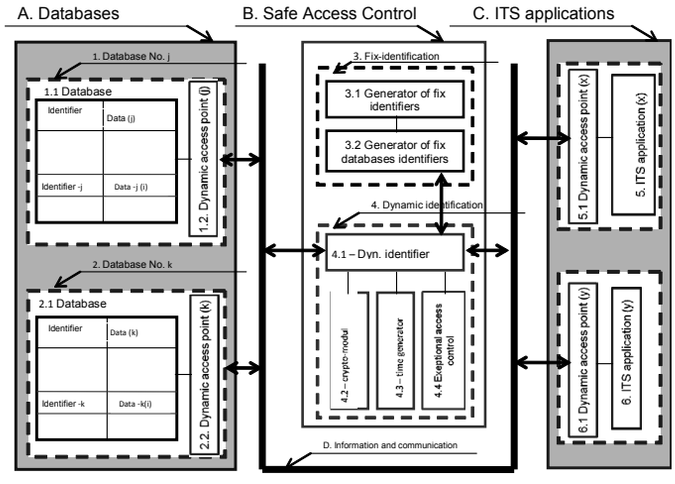

Fig.1. Diagram of the safe access control system into distributed databases

Technically we must guarantee the synchronization of dynamical identifier generator (4.1) with databases access points (1.2), (2.2) and application access points (5.1), (6.1). Databases' access point must transform dynamical identifiers (4.1) into fix databases' identifiers (3.2), select requested data elements, assigned to them dynamical identifiers (4.1) and send them through channel (D).

Dynamical access point in ITS applications connect data from different databases and if the ITS application is authorized to process the connected information the requested information is given to ITS application. The provided data transactions are continuously monitored and each data request and response is recorded.

3. Illustrative example

We would like to show the applicability of the new safe access control system into different databases on practical example of e-Government system in the Czech Republic.

ITS area is planned to be integral part of e-Government information and telecommunication system. For a lot of ITS applications there is necessary to use private sensitive data of inhabitants – e.g. car owners, toll collection data, car licence plates, etc. It is supposed that personal data will be stored in one database, car licence plates in second database, car owners' data in third database, insurance data in fourth database, etc. Each database can be used because identifiers do not carry information about persons.

Only selected ITS applications should connect above mentioned data and make their processing. For example, we can check through ITS application if driver is authorized to drive, if all insurance and financial liabilities of selected person are settled, if the driver is also car owner, etc. How to overcome the "Big brother" problem?

For the ITS applications mentioned above fixed, unique identifier assigned into person is used (we call the unique personal number ZIFO– this number is assigned into each person). The set of fix identifiers are generated from unique ZIFO number with help of generating algorithm – for each database or application the fix identifiers assigned into ZIFO number are used. We call the set of fix identifiers AIFO numbers – for first database/application we have fix identifier AIFO(1), for second database AIFO(2), etc. So we achieve the "static table" of AIFO identifiers generated from unique ZIFO numbers and assigned into different spatially distributed databases or applications.

The new principle of safe access control yields into dynamical component extension (time dependency) and encryption. We can assume that we have two databases (or

similarly ITS applications) x and y, where x-database use AIFO(x) set of identifiers and y-database AIFO(y) set of identifiers. There is request for subsystem (B) for connection of both databases' identifiers – it means the transformation of identifiers AIFO(x) into AIFO(y) in safe way. This typical task is settled in subsystem (B) by two request and response messages.

1. Request message:

$$Z1 = E_K\ (AIFO(x)\ \ ll\ Ti, KA_x, KA_y)$$

where:
E_K = symmetric encryption with key K
Ti = clock state in time of message request
KA_x, KA_y = identification of x- and y-databases
AIFO(x) ll Ti = x-database identifier with link to request time

After receiving the request by system (B), the message Z1 is decoded, AIFO(x) is read and „static table" of identifiers (3.2 on fig.1) is used to generate AIFO(y). The requested AIFO(y) is sent to ITS application in following message form:

2. Response message:

$$Z2 = EK\ (AIFO(y)\ ll\ Ti, ll\ Tj, KA_y, KA_x)$$

where :
E_K = symmetric encryption with key K
Ti = clock state in time of message request
Tj = clock state in time of message response
KA_x, KA_y = identification of x- and y-databases
AIFO(y) ll Ti ll Tj = y-database identifier with link to request and response time

From the example mentioned above it is evident that there exists unique key generated only for one transaction because it is time dependent. The protocol Z1, Z2 was defined only in theoretical level but it came from Hughes variant of Diffie-Hellman protocol of key exchange. The extended variant of this approach can be efficient also for three or more users. It enables multi-connections among the system (B), set of databases (A) and also set of ITS applications (C). The presented multi-points communication is safe and unique for each transaction and fulfill the requested safety requirements [3,4].

4. Conclusion

We presented the first approach into safe access control system into spatially distributed databases. This very new area is theoretically and also practically interesting and can contribute into overcoming very popular, known and discussed "big brother" problem.

It is evident that future development of ITS applications will bring the request for storing and processing more and more data sets. The researchers should concentrate their effort not only to develop new and new applications but also on the problem of safe access control into personal or sensitive data and on the methods of future management of sensitive data processing.

Dynamical identifiers can partly cover this gap and protect the sensitive information against communication channel monitoring by unauthorized person. This approach is now analyzed and tested in newly created "e-Ident laboratory" at Faculty of Transportation Sciences (www.e-Ident.cz) within project 2A-2TP1/108 supported by Ministry of Industry and Trade of the Czech Republic.

Bibliography

[1] JIROVSKÝ, V., et al.: Hybrid Solution of Interoperable European Toll Service, In: Transactions on Transport Sciences. 2008, vol. 1, no. 4, p. 165-174. ISSN 1802-971X.

[2] MOOS, P., SVÍTEK, M., VOTRUBA, Z.: Information Power in Intelligent Transport Systems, In: Transactions on Transport Sciences. 2008, vol. 1, no. 4, p. 193-202. ISSN 1802-971X.

[3] MASTORAKIS N. (ed.): Computers and Simulation in Modern Science, Vol.2, WSEAS Press 2008, ISBN: 978-960-474-032-1, (Zelinka T., Svítek M.: Adaptive wireless access solutions in transport environment, pp. 234-2241.)

[4] ZELINKA, T. SVÍTEK, M.: Multi-path communications access decision scheme, Proceedings of the 12-th World Multi-Conference on Systemics, Cybernetics and Informatics,. Orlando: IIIS - International Institute of Informatics and Systemics, 2008, vol. III, p. 233-237. ISBN 978-1-934272-33-6.