DOI azonosító: 10.17625/NKE.2012.005

ZRÍNYI MIKLÓS
NATIONAL DEFENSE UNIVERSITY
Doctorate Council

THESES OF DOCTORAL (PHD) DISSERTATION

RITA FLEINER

The role and the realization of database security in critical information infrastructure protection

Author's summary and official reviews of PhD dissertation titled

Scientific supervisors:

Prof. Dr. Sándor Munk, DSc
Dr. Lajos Muha, PhD

Budapest
2011

DOI azonosító: 10.17625/NKE.2012.005

1. SCIENTIFIC PROBLEM

By the spread of the information society and the extensive use of information services the role of critical information infrastructure protection is continuously growing. In our days developed societies increasingly depend on different (energetic, communication, information, transport, supply, etc.) infrastructures, and as a consequence, social, economical and every day processes are more and more threatened in case of disruption of the most important – so called critical - infrastructure services. Operation of critical infrastructures nowadays is practically unthinkable without the support of IT systems, applications; therefore critical infrastructures can be threatened through supporting IT systems, and their components, such as databases.

In our days database management systems and the data stored in them play a significant, occasionally crucial role in the operation of many information systems. Violation of the security of databases (attacking the availability, integrity or confidentiality of the stored data or the system) threatens the security of the entire IT system and the services offered by them. From this point of view the implementation, the regulation and the support of database security plays an important role.

In the electronic government it is necessary and crucial to provide data supply in a large volume from electronic registers for the public administration organs, for the local authorities, for entitled business participants and for citizens as well. In our days the fulfilment of public administration services on a high level is impossible without secure, reliable and precise database management.

Although there are several national regulations, proposals and laws for the general and complex protection of the IT systems in the Hungarian e-government, there is further need for the protection of specialized security areas (such as database systems) by specialized security controls, guides and regulations, especially in mission critical applications and systems. Although there are several mission critical database systems in the Hungarian e-government, the regulation of database security in the Hungarian government is still missing.

2. RESEARCH OBJECTIVES

General objective of my research is to analyse and to develop the role, the threats and regulation methods of database security, especially in the field of critical information infrastructure protection and electronic government. Within that I identified the following objectives:

DOI azonosító: 10.17625/NKE.2012.005

- To reveal the basis and the different interpretations of database security. To analyse the architecture of IT systems containing databases and to define the taxonomy of database security threats.
- To analyse, systematize and evaluate the presence, the scope and the role of databases in different critical infrastructure sectors.
- To reveal the present scope and structure of the database security regulation in the Hungarian public administration.
- To outline the possible design directions and documentation structure of the database security regulation in the Hungarian electronic government.

3. NEW SCIENTIFIC RESULTS (THESES)

1. I developed the taxonomy of database security threats according to the place of the attack in the IT architecture.
2. I developed the systematization and evaluation of the scope and the role of databases in different critical infrastructure sectors
3. I introduced the concept of critical databases and I defined their identification method.
4. I proposed a possible design and determined feasible development directions for the Hungarian database security regulation in the public administration.
5. I developed a database security guide that can be used in the Hungarian electronic government.

4. RESEARCH METHODS

In order to fulfil my research goals, I studied the available scientific and informational material, the related PhD theses and books and articles (in paper and in internet as well) related to my research topic. I reviewed the Hungarian and international laws, standards, proposals related to my research topic. Based on the literature studies I performed analysis, I drew conclusions and I brought forward proposals. I conducted personal discussions, interviews with experts working in the field of my research topic and I participated in several conferences and workshops related to my interest. I processed, evaluated and analysed the information and experiences gained during the research. In order to achieve my research goals, during my work I performed systematization, critical adaption, second analysis of other researches and I processed the gathered information and their relationships with the method of analysis and synthesis.

DOI azonosító: 10.17625/NKE.2012.005

5. RESEARCH PERFORMED AND SUMMARY CONCLUSIONS

My PhD dissertation consists of four chapters. In the first one I analyzed the different interpretations of the term ‘database security’ and the changes of its meaning during the time, I revealed the relationship between information system security and database security, I defined the scope and the role of database security within IT security and finally I gave my own definition for database security. In the scope of the definition of ‘database security’ I defined the subject and its security attributes. I consider the database management system and the data stored by them as the subject of database security, and integrity, availability and confidentiality as its primary security attributes. I concluded that database security is an important subfield of information system security which can be accomplished only by taking care of the security of the other parts of the IT systems as well.

Furthermore I analyzed the architectures and components of information technology systems containing databases, I revealed various database security threats by giving several possible aspects for their systematization and I gave taxonomy for the database vulnerabilities. Regarding the implementation of database- and information technology system assurance I find the database vulnerability systematization according to the attack point the most valuable. Within this systematization I gave four categories of the possible attacks: the network, the applications, the platform and the database system.

In the second chapter I summarized the various concepts, attack methods and protection possibilities related to critical infrastructures and I analyzed the identification methodologies of critical infrastructures. I revealed, systematized and gave an overall analysis of the presence and role of databases in different critical infrastructure sectors. I introduced the concept of critical databases and I revealed their identification method.

I found that in ICT services the essential databases play a significant, occasionally crucial role and the violation of their security would come with nationwide affect. In critical infrastructures there are databases, which security is a core component of the security of the given critical infrastructure. For these kinds of databases I proposed to introduce the concept of critical databases. I described two methods to define and qualify critical databases. The first method builds on critical services. It requires the identification of critical services first, after this it becomes possible to find the critical databases belonging to these services. The second method starts from the databases themselves, examines their attributes and draws consequences from these attributes for the criticality.

DOI azonosító: 10.17625/NKE.2012.005

In the third chapter I analyzed the structure of the Hungarian electronic government and the presence and role of databases in it. I analyzed the regulation of information security in the Hungarian public administration and I revealed the absence of database security regulation in it. Although within the e-government information systems databases play a significant role, national laws and proposals regulating the security of e-government don't contain specific rules regarding their security. Government directive 223/2009 regulating the security of national information technology services does have some rules affecting database security, thus for a future national database security regulation this directive can stand as a basic framework.

At last I presented the regulation of database security by analyzing the information assurance controls in the US Armed Forces. I described the technical implementation of database security and analysed the practises and techniques feasible for adoption in the Hungarian national critical infrastructure protection.

In the fourth chapter I analyzed the structure and the role of database security guides and checklists and I proposed a possible design for the Hungarian database security regulation and its development principles. In this framework I proposed to establish a national information assurance centre, whose scope of duties should contain supervisory and implementation elements regarding database security as well.

I propose to develop a multi level based database security regulation. On one level there would stand a Database Security Guide, which should be independent from the actual database management system type and from the working environment. It would contain an ordered list of security controls and it would be issued by a central governmental organization. The other level of the regulation would compose of organization specific documents. The given organization subjected to the regulation should adopt the first level Guide to its own system and environment; this adopted document would be the generic Database Security Guide of the organization. Furthermore the organization should develop its own Database Security Checklist by converting the generic security controls into specific, database system and environment dependent controls. These two documents would compose the Database Security Standard of the specific organization. At the end of the chapter I presented a database security guide developed by the author that can be applied in the Hungarian electronic government and in the Hungarian Critical Information Infrastructure Protection.

DOI azonosító: 10.17625/NKE.2012.005

7. PRACTICAL APPLICATION OF RESEARCH RESULTS, SUGGESTIONS

I suggest to use my PhD Thesis and research results for the following:

1. In the future identification process of the critical databases,
2. In the development of the database security regulation within the Hungarian electronic government,
3. In the implementation of the IT security the presented Database Security Guide can be applied.
4. My thesis can be used for further research of the field ‘critical information infrastructure protection’.
5. My thesis can be used in bachelor, master and doctoral training curriculum in the field of critical information infrastructure protection, database security and electronic government.